



Release Notes for Cisco IOS Release 15.1M&T

First Published: March 26, 2010

Last Updated: September 19, 2013

Release: Cisco IOS Release 15.1(4)M7

Part Number: OL-22146-04 Rev. P0

These release notes support Cisco IOS Release 15.1M&T up to and including Cisco IOS Release 15.1(4)M7. They are updated to describe new features and related documents.

Cisco IOS Release 15.1M&T integrates a portfolio of over 2000 key capabilities that span multiple technology areas, including Security, Voice, Multiprotocol Label Switching (MPLS), IP Services, and Embedded Management.

Key highlights of Cisco IOS Release 15.1M&T include the following:

- Ideal for very latest features and hardware support.
- Incorporates features and hardware support previously delivered in Cisco IOS Release 15.0(1)M and prior releases.
- Positioned for short deployment cycle (until next Extended Maintenance release becomes available).
- Standard maintenance bug-fix rebuild for 13 months, plus an additional 6 months support for security/vulnerability issues such as Cisco Product Security Incident Response Team (PSIRT) advisories (see http://www.cisco.com/en/US/products/products_security_advisories_listing.html).
- Rebuilds of Cisco IOS Release 15.1M&T that contain bug fixes only.

Contents

This document contains the following sections:

- [Cross-Platform System Requirements, page 2](#)
- [MIBs, page 4](#)
- [Field Notices and Software-Related Tools and Information, page 4](#)
- [Troubleshooting, page 4](#)

Cross-Platform System Requirements

This section describes the system requirements for Cisco IOS Release 15.1M&T and includes the following sections:

- [Supported Hardware Platforms, page 2](#)
- [Determining Your Software Version, page 3](#)
- [Upgrading to a New Release, page 3](#)

Supported Hardware Platforms

Cisco IOS Release 15.1M&T supports the following Cisco hardware platforms:

- Cisco 800 series routers
- Cisco 1800 series routers
- Cisco 1900 series integrated services routers
- Cisco 2800 series integrated services routers
- Cisco 2900 series integrated services routers
- Cisco 3800 series integrated services routers
- Cisco 3900 series integrated services routers
- Cisco AS5350XM universal gateways
- Cisco AS5400XM universal gateways
- Cisco CGR 2000 series
- Cisco IAD2430 series integrated access devices
- Cisco IAD2801 series integrated access devices
- Cisco unified communications 500 series
- Cisco VG200 series analog voice gateways
- Cisco VGD 1 T3 voice gateways

**Note**

Cisco 7200 series and Cisco 7301 routers will continue to be supported in Cisco IOS 15.n(n)M releases. Only the Cisco IOS 15.n(n)T releases will not support the Cisco 7200 series and Cisco 7301 routers.

For more information about the platforms supported in Cisco IOS Release 15.1M&T, see the “Platform-Specific Information” section on page 10.

Determining Your Software Version

To determine the version of Cisco IOS software that is currently running on your Cisco network device, log in to the device and enter the **show version** user EXEC command:

```
Router> show version
```

```
Cisco Internetwork Operating System Software IOS (tm)  
15.1 Software (c2430-is-mz), Version 15.1(1)T, RELEASE SOFTWARE
```

Upgrading to a New Release

For information about selecting a new Cisco IOS software release, see *How to Choose a Cisco IOS Software Release* at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

For information about upgrading to a new software release, see the appropriate platform-specific documents:

- Cisco VG202, Cisco VG204, Cisco VG224
http://www.cisco.com/en/US/products/hw/gatecont/ps2250/prod_installation_guides_list.html
- Cisco 800 series routers
http://www.cisco.com/en/US/products/hw/routers/ps380/prod_installation_guides_list.html
- Cisco 1800 series routers
http://www.cisco.com/en/US/products/ps5853/prod_installation_guides_list.html
- Cisco 2800 series routers
http://www.cisco.com/en/US/products/ps5854/prod_installation_guides_list.html
- Cisco 3800 series routers
http://www.cisco.com/en/US/products/ps5855/prod_installation_guides_list.html
- Cisco AS5350XM series universal gateways
http://www.cisco.com/en/US/products/hw/univgate/ps501/prod_installation_guides_list.html
- Cisco AS5400XM series universal gateways
http://www.cisco.com/en/US/products/hw/univgate/ps501/prod_installation_guides_list.html

For instructions on ordering a Cisco IOS upgrade, see the document at the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Field Notices and Software-Related Tools and Information

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at

<http://www.cisco.com/cisco/software/navigator.html>.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*
http://www.cisco.com/en/US/products/hw/routers/ps214/products_tech_note09186a008012fb88.shtml
- *Troubleshooting Bus Error Exceptions*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml
- *Why Does My Router Lose Its Configuration During Reboot?*
http://www.cisco.com/en/US/products/hw/routers/ps233/products_tech_note09186a00800a65a5.shtml

- *Troubleshooting Router Hangs*
http://www.cisco.com/en/US/products/hw/routers/ps359/products_tech_note09186a0080106fd7.shtml
- *Troubleshooting Memory Problems*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6f3a.shtml
- *Troubleshooting High CPU Utilization on Cisco Routers*
http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a70f2.shtml
- *Troubleshooting Router Crashes*
http://www.cisco.com/en/US/products/hw/iad/ps397/products_tech_note09186a00800b4447.shtml
- *Using CAR During DOS Attacks*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a00800fb50a.shtml

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains specific Cisco IOS features.



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Feature-to-image mapping is available through Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). You can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

www.cisco.com/go/cfn

For help with Cisco Feature Navigator, see the help information at the following URL:

http://www.cisco.com/web/applicat/CFNTOOLS/Help_Docs/help/cfn_support.html

Determining the Software Images (Feature Sets) That Support a Specific Feature

To determine which software images (feature sets) in a Cisco IOS release support a specific feature, go to the [Cisco Feature Navigator home page](#) and perform the following steps.

- Step 1** From the Cisco Feature Navigator home page, click **Research Features**.
- Step 2** Select your software type or leave the field as "All".
- Step 3** To find a feature, you can search by either Feature or Technology (select the appropriate button). If you select Search by Feature, you can further filter your search by using the Filter By text box.
- Step 4** Choose a feature from the Available Features text box, and click the **Add** button to add the feature to the Selected Features text box.



Note

To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Repeat this step to add features. A maximum of 20 features can be chosen for a single search.

- Step 5** Click **Continue** when you are finished choosing features.

- Step 6** In the Release/Platform Tree area, select either your release (from the Train-Release list) or your platform (from the Platform list).
- Step 7** The “Search Result” table will list all the software images (feature sets) that support the features that you chose.



Note You can download your results into an Excel spreadsheet by clicking on the Download Excel button.

Determining the Features Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set), go to the [Cisco Feature Navigator home page](#) and perform the following steps.

- Step 1** From the Cisco Feature Navigator home page, click **Research Software**.
- Step 2** Select your software type from the drop-down list and chose the **Release** button in the “Search By” area.
- Step 3** From the Major Release drop-down list, chose the appropriate major release.
- Step 4** From the Release drop-down list, choose the appropriate maintenance release.
- Step 5** From the Platform drop-down list, choose the appropriate hardware platform.
- Step 6** From the Feature Set drop-down list, choose the appropriate feature set. The Image Details area will provide details on the specific image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.



Note To learn more about a feature in the list, click the **View Desc** button in the Available Features text box.

Memory Recommendations

To determine memory recommendations for software images (feature sets) in your Cisco IOS release, go to the [Cisco Feature Navigator home page](#) and perform the following steps.

- Step 1** From the Cisco Feature Navigator home page, click **Research Software**.
- Step 2** Select your software type from the drop-down list and choose the **Release** button in the “Search By” area.
- Step 3** From the Major Release drop-down list, choose the appropriate major release.
- Step 4** From the Release drop-down list, choose the appropriate maintenance release.
- Step 5** From the Platform drop-down list, choose the appropriate hardware platform.
- Step 6** From the Feature Set drop-down list, choose the appropriate feature set.

- Step 7** The Image Details area will provide details on the specific image including the DRAM and flash memory recommendations for each image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.
-

Platform-Specific Information

This section describes the platform-specific information for the following Cisco platforms supported by Cisco IOS Release 15.1M&T:

- [Cisco 800 Series Routers, page 11](#)
- [Cisco 1800 Series Routers \(Fixed Configuration and Modular\), page 12](#)
- [Cisco 1900 Series Integrated Services Routers, page 13](#)
- [Cisco 2800 Series Integrated Services Routers, page 14](#)
- [Cisco 2900 Series Integrated Services Routers, page 15](#)
- [Cisco 3800 Series Integrated Services Routers, page 16](#)
- [Cisco 3900 Series Integrated Services Routers, page 17](#)
- [Cisco 7200 Series Routers, page 18](#)
- [Cisco AS5350XM Universal Gateways, page 19](#)
- [Cisco AS5400XM Universal Gateways, page 20](#)
- [Cisco Connected Grid Router 2000 Series, page 21](#)
- [Cisco IAD2430 Series Integrated Access Devices, page 22](#)
- [Cisco IAD2801 Series Integrated Access Devices, page 23](#)
- [Cisco VG200 Series Analog Voice Gateways, page 24](#)
- [Cisco VGD 1T3 Voice Gateways, page 25](#)

Cisco 800 Series Routers

Cisco IOS Release 15.1M&T supports the Cisco 800 series routers.

Introduction

For detailed information about the Cisco 800 series of routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/hw/routers/ps380/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 800 series routers:

- Cisco 819G, Cisco 819HG
- Cisco 860 (Cisco 861, Cisco 866, Cisco 866 VAE, Cisco 867, Cisco 867 VAE) (Cisco 860 series ISG introduced in Cisco IOS Release 15.1(4)M2)
- Cisco 870 (Cisco 871, Cisco 876, Cisco 877, Cisco 878)
- Cisco 881 (Cisco 881, Cisco 881 CUBE, Cisco 881W, Cisco IAD881, Cisco SRST881)
- Cisco 886 (Cisco 886, Cisco 886 CUBE, Cisco IAD886, Cisco 886 VA, Cisco 886 VA-W)
- Cisco 887 (Cisco 887, Cisco 887 CUBE, Cisco IAD887, Cisco 887 VA, Cisco 887 VA-M, Cisco 887 VA-W, Cisco 887 VAM-W)
- Cisco 888 (Cisco 888, Cisco 888 CUBE, Cisco 888E, Cisco IAD888, Cisco SRST888)
- Cisco 890 (Cisco 891, Cisco 892, Cisco 892F CUBE)

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco 1800 Series Routers (Fixed Configuration and Modular)

Cisco IOS Release 15.1M&T supports the Cisco 1800 series routers.

Introduction

For detailed information about the Cisco 1800 series integrated service routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps5853/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 1800 series routers:

- Cisco 1801, Cisco 1802, Cisco 1803, and Cisco 1805, wireless and nonwireless
- Cisco 1811 and Cisco 1812, wireless (fixed configuration)
- Cisco 1811 and Cisco 1812, nonwireless (fixed configuration)
- Cisco 1841, Cisco 1841 VE (modular)
- Cisco 1841C (The Cisco 1841C router is supported in Cisco IOS Release 15.1(1)T1 and later releases.)
- Cisco 1861, Cisco 1861E (integrated services)

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/ps5853/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco 1900 Series Integrated Services Routers

Cisco IOS Release 15.1M&T supports the Cisco 1900 series routers.

Introduction

For detailed information about the Cisco 1900 series integrated service routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps10538/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 1900 series integrated services routers:

- Cisco 1905
- Cisco 1906C
- Cisco 1921
- Cisco 1941
- Cisco 1941W

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/ps10538/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco 2800 Series Integrated Services Routers

Cisco IOS Release 15.1M&T supports the Cisco 2800 series integrated service routers.

Introduction

For detailed information about the Cisco 2800 series integrated service routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps5854/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 2800 series integrated services routers:

- Cisco 2801
- Cisco 2801C (The Cisco 2801C router is supported in Cisco IOS Release 15.1(1)T1 and later releases.)
- Cisco 2811, Cisco 2811 VE
- Cisco 2811C (The Cisco 2811C router is supported in Cisco IOS Release 15.1(1)T1 and later releases.)
- Cisco 2821
- Cisco 2821C (The Cisco 2821C router is supported in Cisco IOS Release 15.1(1)T1 and later releases.)
- Cisco 2851

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/ps5854/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

**Note**

The minimum DRAM to run c2801-adventerprisek9-mz in Cisco IOS Release 15.1M&T is 192 MB.

Cisco 2900 Series Integrated Services Routers

Cisco IOS Release 15.1M&T supports the Cisco 2900 series integrated service routers.

Introduction

For detailed information about the Cisco 2900 series of routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps10537/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 2900 series integrated services routers:

- Cisco 2901
- Cisco 2911
- Cisco 2921
- Cisco 2951

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/ps10537/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco 3800 Series Integrated Services Routers

Cisco IOS Release 15.1M&T supports the Cisco 3800 series integrated service routers.

Introduction

For detailed information about the Cisco 3800 series of routers, see the documents at the following location:

http://www.cisco.com/en/US/products/ps5855/tsd_products_support_series_home.html

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 3800 series integrated services routers:

- Cisco 3825
- Cisco 3825-NOVPN
- Cisco 3845
- Cisco 3845-NOVPN

For information about the interfaces and modules for this platform, see the following document:

<http://www.cisco.com/en/US/docs/routers/access/3800/hardware/notes/3800ioh.html>

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco 3900 Series Integrated Services Routers

Cisco IOS Release 15.1M&T supports the Cisco 3900 series integrated service routers.

Introduction

For detailed information about the Cisco 3900 series of routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps10536/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 3900 series integrated services routers:

- Cisco 3925
- Cisco 3925E
- Cisco 3945
- Cisco 3945E

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/ps10536/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco 7200 Series Routers

Cisco IOS Release 15.1M&T supports the Cisco 7200 series routers.

Introduction

For detailed information about the Cisco 7200 series of routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/hw/routers/ps341/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco 7200 series routers:

- Cisco 7200
- Cisco 7200-NPE-G2
- Cisco 7201
- Cisco 7301

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/hw/routers/ps341/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco AS5350XM Universal Gateways

Cisco IOS Release 15.1M&T supports the Cisco AS5350XM universal gateways.

Introduction

For detailed information about the Cisco AS5350XM universal gateway, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps6268/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the Cisco AS5350XM universal gateways.

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco AS5400XM Universal Gateways

Cisco IOS Release 15.1M&T supports the Cisco AS5400XM universal gateways.

Introduction

For detailed information about the Cisco AS5400XM universal gateway, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps6269/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the Cisco AS5400XM universal gateways.

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco Connected Grid Router 2000 Series

Cisco IOS Release 15.1M&T supports the Cisco connected grid router 2000 series.

Introduction

For detailed information about Cisco Connected Grid Routers, see the documents at the following location:

<http://www.cisco.com/en/US/products/ps10977/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the Cisco Connected Grid Router 2010 (CGR 2010).

For information about the interfaces and modules for this platform, see the following document:

http://www.cisco.com/en/US/products/ps10977/products_relevant_interfaces_and_modules.html

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco IAD2430 Series Integrated Access Devices

Cisco IOS Release 15.1M&T supports the Cisco IAD2430 series integrated access devices.

Introduction

For detailed information about the Cisco IAD2430 series integrated access devices, see the documents at the following location:

<http://www.cisco.com/en/US/products/hw/gatecont/ps887/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco IAD2430 series integrated access devices:

- Cisco IAD2430
- Cisco IAD2431
- Cisco IAD2432
- Cisco IAD2435

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco IAD2801 Series Integrated Access Devices

Cisco IOS Release 15.1M&T supports the Cisco IAD2801 series integrated access devices.

Introduction

For detailed information about Cisco IAD2801 series integrated access devices, see the documents at the following location:

http://www.cisco.com/en/US/products/ps7214/tsd_products_support_series_home.html

Supported Hardware

Cisco IOS Release 15.1M&T supports the Cisco IAD2801 series integrated access devices.

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco VG200 Series Analog Voice Gateways

Cisco IOS Release 15.1M&T supports the Cisco VG200 series analog voice gateways.

Introduction

For detailed information about the Cisco VG200 series analog voice gateways, see the documents at the following location:

<http://www.cisco.com/en/US/products/hw/gatecont/ps2250/index.html>

Supported Hardware

Cisco IOS Release 15.1M&T supports the following Cisco VG200 series analog voice gateways:

- Cisco VG202
- Cisco VG204
- Cisco VG224

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.

Cisco VGD 1T3 Voice Gateways

Cisco IOS Release 15.1M&T supports the Cisco VGD 1T3 series voice gateways.

Introduction

For detailed information about the Cisco VGD 1T3 series voice gateways, see the documents at the following location:

http://www.cisco.com/en/US/products/ps9890/tsd_products_support_series_home.html

Supported Hardware

Cisco IOS Release 15.1M&T supports the Cisco VGD 1T3 series voice gateways.

For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Memory recommendations and feature support information for Cisco IOS Release 15.1M&T are also available through Cisco Feature Navigator.



Features and Important Notes for Cisco IOS Release 15.1(1)T

Contents

These release notes describe the following topics:

- [New and Changed Information, page 27](#)
- [Important Notes, page 39](#)

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1M&T and contains the following subsections:

- [New Hardware Features Supported in Cisco IOS Release 15.1\(1\)T5, page 27](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(1\)T5, page 28](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(3\)T3, page 28](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(1\)T4, page 28](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(1\)T1, page 28](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(1\)T1, page 29](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(1\)T, page 29](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(1\)T, page 31](#)



Note

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at <http://www.cisco.com/go/cfn>.

New Hardware Features Supported in Cisco IOS Release 15.1(1)T5

There are no new hardware features in Cisco IOS Release 15.1(1)T5.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New Software Features Supported in Cisco IOS Release 15.1(1)T5

There are no new software features in Cisco IOS Release 15.1(1)T5.

New Hardware Features Supported in Cisco IOS Release 15.1(3)T3

There are no new hardware features in Cisco IOS Release 15.1(3)T3.

New Software Features Supported in Cisco IOS Release 15.1(1)T4

This section describes new and changed features in Cisco IOS Release 15.1(1)T4. Some features may be new to Cisco IOS Release 15.1(1)T4 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(1)T4. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Right To Use Licensing Support in CLIs and MIBs for Cisco ISR G2 Platforms

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

New Hardware Features Supported in Cisco IOS Release 15.1(1)T1

This section describes new and changed features in Cisco IOS Release 15.1(1)T1. Some features may be new to Cisco IOS Release 15.1(1)T1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(1)T1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

1-Port and 2-Port VWIC3s—Voice WAN Interface Cards

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/vd-t1e1_vwic3.html

Cisco Integrated Service Routers Generation 1 C-Series

Cisco IOS Release 15.1(1)T1 supports the Cisco 1841C, Cisco 2801C, Cisco 2811C, Cisco 2821C, Cisco 3825C, and Cisco 3845C integrated service routers generation 1 C-series. The following features are not supported on these routers:

- Cisco Communications Manager Express (CCME)
- Cisco Unified Border Element (CUBE)
- Dynamic Multipoint Virtual Private Network (DMVPN)
- Group Encrypted Transport Virtual Private Network (GET-VPN)
- Hierarchical Quality of Service (HQoS)
- Multicast features:
 - PIM SSM
 - IGMPv3
 - MVPN
 - MSDP
- Netflow v9
- Optimized Edge Routing (OER)
- Performance Routing (PFR)
- Power over Ethernet (PoE)
- Survivable Remote Site Telephony (SRST)

New Software Features Supported in Cisco IOS Release 15.1(1)T1

This section describes new and changed features in Cisco IOS Release 15.1(1)T1. Some features may be new to Cisco IOS Release 15.1(1)T1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(1)T1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Voice Support on 1-Port and 2-Port HWICs

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_11xw/fmt1e1ic_voice.html

New Hardware Features Supported in Cisco IOS Release 15.1(1)T

This section describes new and changed features in Cisco IOS Release 15.1(1)T. Some features may be new to Cisco IOS Release 15.1(1)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(1)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

3G HSPA Enhancement

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/hw/routers/ps380/products_installation_and_configuration_guides_list.html

Cisco 1905 and Cisco 1921 Integrated Service Routers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/1900/hardware/installation/guide/1900_HIG.html

Cisco 3925E and Cisco 3945E Integrated Service Routers

The Cisco 3945E and Cisco 3925E offer new Services Performance Engines (SPEs), that are high-performance modular motherboards with a cryptographic accelerator, 4 onboard GE ports, 2 SFP slots, 3 EHWIC slots, 3 PVDM3 slots, and up to 350Mbps WAN Access with services. The Cisco 3945E and 3925E are shipped with Services Performance Engines (SPEs) pre-installed in the router, or are sold separately. The SPE250 and SPE200 provide a modular approach to system upgrades, because you can easily upgrade the SPE on a Cisco 3945 or Cisco 3925 for improved router performance.

The Cisco 3945E and Cisco 3925E provide highly scalable Security and UC/CUBE services and offer investment protection for customers who purchase a Cisco 3925 or Cisco 3945 today, providing an upgrade option for higher performance levels in the future when increased bandwidth demands require higher performance levels.

Cisco 888E

For detailed information about this feature, see the following documents:

<http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/hardware/installation/guide/860-880-890HIG.html>

<http://www.cisco.com/en/US/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html>

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/dsl_hwic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/oview_ic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_HWICS.html

Cisco Connected Grid Router 2000 Series

The Cisco Connected Grid Router 2010 (Cisco CGR 2010) router is a member of the Cisco Connected Grid Router 2000 Series family of routers. It is an especially rugged, high performance router that provides LAN and WAN connectivity, field replaceable parts, and feature upgrades through software licensing. The Cisco CGR 2010 is designed to withstand hostile environments while continuing to deliver the performance, availability, and reliability to scale mission-critical needs.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/ps10977/products_installation_and_configuration_guides_list.html

Cisco Unified Communications 500 Series

The Cisco Unified Communications 500 Series is part of the Cisco Smart Business Communications System (SBCS). The Cisco UC 500 series is a unified communications solution for small businesses that provides voice, data, video, and security capabilities.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/ps7293/tsd_products_support_series_home.html



Note

Cisco UC 500 images are only available via Cisco UC 500 software packs on the Small Business Community Site at www.cisco.com/go/smallbizsupport.

HWIC-1VDSL

The HWIC-1VDSL is used on the Cisco ISR G2 platforms to provide VDSL over POTs WAN connectivity. It can be installed on Cisco ISR G2 platforms, and the external RJ-11 port is connected to DSL line coming from VDSL2 supported DSLAM.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/ps5949/tsd_products_support_series_home.html

HWIC-4SHDSL-E

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_HWICS.html

New Software Features Supported in Cisco IOS Release 15.1(1)T

This section describes new and changed features in Cisco IOS Release 15.1(1)T. Some features may be new to Cisco IOS Release 15.1(1)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(1)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Call Home

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/callhome_asr1k.html

Call Restriction Regulations

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmelpcor.html

Cisco Unified Border Element Support for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html#wpxref97945>

CME (Communications Manager Express) 8.0/SRST (Survivable Remote Site Telephony) 8.0

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/Cisco_Unified_IPPhones_69xx_Series.html#wp1072892

CME CSTA CTI Protocol Suite

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmecti.html

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/open/source/sdkgnusl.html

Compliance-Mode Cipher and Hash Selection for GET VPN Group Member

This feature allows Federal Information Processing Standards (FIPS) compliance and Common Criteria (CC) compliance by enabling Cisco Group Encrypted Transport VPN (GET VPN) group members to specify locally-acceptable cipher and hash algorithms for the key encryption keys (KEKs) and traffic encryption keys (TEKs) that they download from the key server. This feature is configured with the following commands:

client rekey encryption

client rekey hash

client transform-sets

For detailed information about these commands, see the following document:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

DHCP Zero Touch

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_wsma.html

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Direct Download from CCO Capability in Cisco IOS IPS

The Direct Download from CCO Capability in Cisco IOS IPS feature was introduced to allow an administrator to use the CLI to specify, download and upgrade new signatures posted for Cisco IOS directly from Cisco.com. An administrator can also configure the router through the CLI to receive future periodic signature downloads automatically to eliminate the manual maintenance efforts and costs of changing or tuning IPS signatures whenever a new IPS signature update is posted.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ips5_sig_fs_ue.html

DoD MLPP PBX1 Certification for CME

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmemplpp.html

DoD Secure Device Support for CME: Support STU/STE/IP STE with CME

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmebasic.html

EnergyWise Branch Routers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/products/ps10538/tsd_products_support_configure.html

Enhanced Music on Hold

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmehom.html#wp1022363

G.SHDSL Auto Pair Detect

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/shdslfm.html#wp1054629>

IEEE 802.1ag—D8.1 Standard Compliant CFM, Y.1731 Multicast LBM/AIS/RDI/LCK, IP SLA for Ethernet

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee.html

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_y1731.html

IKEv2 Site-to-Site

IKEv2 is the supporting protocol for IP Security Protocol (IPsec) and is used for performing mutual authentication and establishing and maintaining security associations (SAs). IKEv2 supports crypto-map and tunnel protection based IKEv2 solutions and features such as Dynamic Multipoint VPN (DMVPN), IPsec Static Virtual Tunnel Interface (sVTI), and IPsec Dynamic Virtual Tunnel Interface (dVTI).

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

IP SLAs Engine 3.0

The Auto IP SLAs feature in Cisco IOS IP Service Level Agreements (SLAs) Engine 3.0 enables you to define a single probe definition that can be combined with different collections of endpoints to create multiple operations, including operations for proactive threshold monitoring, and allows a source to auto-discover the endpoints of an IP SLAs Responder. IP SLAs Engine 3.0 also enables the active measurement of Quality of Service (QoS) performance.

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/sla-15-1mt-book.html>

iSAC Codec Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_book/vb_book.html

Key Replacement for Digitally Signed Cisco Software

The Key Replacement for Digitally Signed Cisco Software feature provides a mechanism to replace public keys on a Cisco router or switch that are used to verify the authenticity of the software image.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_dgtly_sgnd_sw.html

Layer 2 Switch Port Manageability MIBs

The Layer 2 Ethernet Switching Interface BRIDGE-MIB is supported in the Cisco 1861 platform. The BRIDGE-MIB enables the user to know the Media Access Control (MAC) addresses and spanning tree information of the Ethernet switch modules. The user can query the MIB agent using the SNMP protocol and get the details of Ethernet switch modules such as MAC addresses of each interfaces and spanning protocol information.

The Bridge-MIB uses the following approaches to get the Layer 2 BRIDGE-MIB information:

- Community string based approach
- Context based approach

In the community string based approach, one community string is created for each VLAN. Based on the query, the respective VLAN MIB is displayed.

In the context based approach, the SNMP context mapping commands are used to display the values for the L2 interfaces information. Each VLAN is mapped to a context. When the user queries with a context, the MIB displays the data for that specific VLAN which is mapped to the context. In this approach, each VLAN is manually mapped to a context.

For more details to configure and retrieve the BRIDGE-MIB details, see the Release Notes and Technical Notes at:

http://www.cisco.com/en/US/docs/ios/15_0/15_0x/15_01_XA/rn1800xa.html#wp422468

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml#brgmib

LDAP Integration with Active Directory

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_accountg.html

LDAP/AD Support for Authproxy

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authentifcn_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1001230

MLPP Support for Supplementary Services on SCCP Controlled Analog Endpoints

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fxshist.html>

MPLS MTU Command for GRE Tunnels

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1mt/mp-any-transport.html

Parser Concurrency and Locking Improvements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-lock.html

QoS Policing Support on Switched Virtual Interfaces (SVIs)

The **police** command was modified to include support for policing on Switched Virtual Interfaces (SVIs) for the Cisco1800, 2800, and 3800 series integrated services routers.

Reuse MAC for ATM RBE

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_reuse_MAC_for_ATM_RBE.html

RFC4040 Based Clear Channel Codec Signaling with SIP

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-rfc_comply.html

RSA 4096-Bit Key Generation in SW Crypto Engine Support

The range value for **the modulus** keyword value for the **crypto key generate rsa** command is extended from 360 to 2048 bits to 360 to 4096 bits.

This change impacts the following Cisco documents:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_deploy_RSA_piki.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_store_pki_cred.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_mng_cert_serv.html

In the following document the **crypto key generate rsa** command was updated:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html

Serviceability Support for SIP Dialer and Call Progress Analysis

Cisco IOS Release 15.1(1)T adds two command line interface (CLI) commands for Call Progress Analysis (CPA) monitoring and diagnostics:

test dsp cpa slot dsp message

This command enables or disables printing of CPA messages to the console or/and the syslog.

test dsp cpa slot dsp parameter

This command displays or resets CPA parameters.

SG3 Fax Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/fax/configuration/guide/vf_cfg_t38_fxrlly.html

SIP—TLS/TCP and SRTP with SRST

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/firmware/8_5_3/english/release/notes/7900_853.html

SIP IPv6—ANAT Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmesystem.html

SSL VPN Phase-4 Features

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn.html

SSLVPN DVTI Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn.html

Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP to SIP Calls

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_10022.html

Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Interworking Between RSVP Capable and RSVP Incapable Networks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_10021.html

Support for MGCP 1.0 Call Control for SRTP on Cisco IOS Gateways

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/mgcp/configuration/guide/15_0/vm_15_0_book.html

Support for MIB to Report Call Volume and Call Rate Related Statistics on the Cisco Unified Border Element

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-roadmap.html>

Support for Multiple Registrars on SIP Trunks on a Cisco Unified Border Element, on Cisco IOS SIP TDM Gateways, and on Cisco Unified Communications Manager Express

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-multi-registrars.html

Support for PAI, PPI and Privacy Headers on the SIP Trunk of CUCME with Either SIP or SCCP Line-Side

Support for PAI, PPI, and Privacy Headers on the Cisco Unified CME SIP trunk. When enabled, Calling Number, Calling Name, and Privacy information is sent using PAI, PPI, and Privacy headers over the SIP trunk of Cisco Unified CME. This feature also enables interworking between the Remote-Party-ID (RPID) information contained in SIP line-side messages to PAI, PPI, and Privacy header information on the SIP trunk.

Support for SIP 181 Call is Being Forwarded Message

Support for SIP 181 Call is Being Forwarded message was added to Cisco IOS SIP TDM gateways and Cisco Unified Border Elements (Cisco UBEs). This feature is enabled by default. To disable this feature for all SIP 181 messages or for SIP 181 message either with or without SDP, see the **block** and **voice-class sip block** commands in the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html.

On the Cisco UBE, this feature also adds the ability to receive SIP 181 messages on one leg and send out SIP 183 messages on the other leg. For details about enabling this feature on a Cisco UBE, see the **map resp-code** and **voice-class sip map resp-code** commands in the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html.

Support for Stripping Off Progress Indication from Incoming ISDN Messages on SIP and H323 TDM Gateways

Support for stripping off progress indicator (PI) from incoming Q.931 CALL-PROCEEDING message on Cisco IOS SIP and H.323 gateways and on Cisco UBEs. Configuration of this feature determines whether an incoming Q.931 CALL-PROCEEDING message with a PI value results in a SIP 183 message or H.323 Progress message. This behavior allows interworking with third-party SIP and H.323 servers. For details about enabling this feature, see the **progress_ind** command in the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html.

Tcl UDP and VRF Support

The Tcl UDP and VRF feature provides support for UDP sockets. This feature also provides VRF support for all Tcl sockets, including both UDP and TCP sockets.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_script_tcl.html

Transport 802.1q and 802.1p Tags over ATM PVCs

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_trans_vlan-tags_dsl_links.html

Web Services Management Agent with TLS

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_wsma.html

Zone Based Firewall (ZBFW) Usability and Manageability Features

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_zone_policy_firew.html

Important Notes

The following information applies to all releases of Cisco IOS Release 15.1(1)T.

- [Cisco IOS Behavior Changes, page 39](#)
- [Important Notes for Cisco IOS Release 15.1\(1\)T, page 45](#)

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- [Cisco IOS Release 15.1\(1\)T5, page 39](#)
- [Cisco IOS Release 15.1\(1\)T4, page 39](#)
- [Cisco IOS Release 15.1\(1\)T3, page 40](#)
- [Cisco IOS Release 15.1\(1\)T2, page 42](#)
- [Cisco IOS Release 15.1\(1\)T1, page 42](#)

Cisco IOS Release 15.1(1)T5

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T5:

- The SIP call hold/resume scenario has been enhanced so that the RTP sequence number is continuous from the origin of the call till the end.

Old Behavior: The RTP sequence number is not continuous from the origin until the end of a SIP call, including the time when the call is on hold.

New Behavior: The RTP sequence number is now continuous from the origin until the end of a SIP call.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-1mt/sip-to-sip_supplementary_services_for_session_border_controller.html

Cisco IOS Release 15.1(1)T4

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T4:

- A CERM license is reserved only after the user logs in.

Old Behavior: A Crypto Export Restrictions Manager (CERM) license is reserved for every SSL or TLS session.

New Behavior: A CERM license is reserved only after the user logs in.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-2mt/sec-conn-sslvpn-ssl-vpn.html#GUID-33399B8A-875B-42E9-BA7F-375F68B64208

Cisco IOS Release 15.1(1)T3

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T3:

- BGP address families no longer stuck in NoNeg or idle state after reload.

Old Behavior: After a reload of a router, some or all of the BGP address families do not come up. This is because the router is receiving messages from a neighbor that the AFI or SAFI is not supported, and the router does not retry those AFIs. The output of **show ip bgp all summary** shows the address family in NoNeg or idle state, and it will never leave that state. Typical output looks like:

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
x.x.x.x 4 1 0 0 1 0 0 never (NoNeg)
```

New Behavior: When the router receives a message that the AFI or SAFI is not supported, the router does not simply drop the rejected AFIs or SAFIs from subsequent OPEN messages. Instead, the router retries the AFI/SAFI within the existing OPEN message retry timing sequence, but with an exponential backoff (stopping at 10 minutes) applied to decisions about whether to include a particular AFI/SAFI in an OPEN message. The timing of OPEN messages is not changed. Successful negotiation of the AFI results in a reset of the backoff sequence for future attempts. Also, when a BGP connection collision occurs with a session in the ESTABLISHED state, BGP sends a CEASE notification on the newly opened connection, and a keepalive message on the old connection. The new connection is closed. If the old session was stale, the keepalive causes it to be closed. The neighbor will retry its OPEN message after receiving the CEASE message and waiting a few seconds.

- New BGP Error Message.

Old Behavior: No error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels (via the neighbor send-label command or via a template). Sending MPLS labels to IPv6 peers is not supported.

New Behavior: An error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels. An example of the error message is:

```
"%BGP-4-BGP_LABELS_NOT_SUPPORTED: BGP neighbor 2001:DB8:1::2 does not support sending labels."
```

- The summary address is not advertised to the peer.

Old Behavior: The summary address is advertised to the peer if the administrative distance is configured as 255.

New Behavior: The summary address is not advertised to the peer if the administrative distance is configured as 255.

- TCP keepalive sessions are terminated when a host behind a zone-based policy firewall disconnects ungracefully.

Old Behavior: When a host behind a zone-based policy firewall disconnects ungracefully and loses the TCP connection information, TCP keepalive sessions are terminated on the other endpoint after the TCP keepalive times out.

New Behavior: When a zone-based policy firewall is enabled for TCP keepalive traffic and the host behind the firewall is undergoing an ungraceful disconnect, TCP keepalive works only when the configured TCP timeout is complete. On receiving an out of window reset (RST) packet, the firewall sends an empty acknowledge (ACK) packet to the initiator of the RST packet. This ACK will have the current sequence (SEQ) and ACK number from the firewall session. On receiving this ACK, the client sends an RST packet with the SEQ number that is equal to the ACK number in ACK packet. The firewall processes this RST packet, clears the firewall session, and passes the RST packet.

Additional Information:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_zone_policy_firew.html

- Two new keywords, *protocol* and *pbr*, are added to the **mode route** command.

Old Behavior: Destination-only traffic classes cannot be controlled when more than one protocol is operating at the border routers.

New Behavior: Destination-only traffic classes can be controlled when more than one protocol is operating at the border routers using dynamic PBR.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html>

- On Cisco 860, 880, 890, 2900, and 3900 series ISRs, the default behavior changes when the interface is not connected to an active port:

Old Behavior: GigabitEthernet0/3/0 is up, line protocol is down.

New Behavior: GigabitEthernet0/3/0 is down, line protocol is down.

- The line coding and loss of sync information is changed in the output for the **show controller shdsl** command.

Old Behavior: The output for the **show controller shdsl** command for the HWIC- 4SHDSL-E shows the line coding as AUTO-TCPAM when Annex F and G are selected, and loss of sync as LOSWAS.

New Behavior: The output for the **show controller shdsl** command for the HWIC- 4SHDSL-E shows the line coding as 16-TCPAM or 32-TCPAM depending on which TCPAM is used to train lines when Annex F and G are selected, and loss of sync as LOSW.

Additional Information:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_HWICS.html

- New keyword added to **ignore crc** command.

Old Behavior: The *always* keyword was not available for the **ignore crc** command.

New Behavior: The **ignore crc** command can use the *always* keyword to always ignore CRC errors.

Additional information:

http://www.cisco.com/en/US/docs/ios/bbdsi/command/reference/bba_book.html

- New command, **ntp panic update**, is introduced

Old Behavior: There is no command to configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds.

New Behavior: A new command, **ntp panic update**, is introduced to configure NTP to reject time updates greater than the panic threshold of 1000 seconds. If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000. seconds; set clock manually to the correct UTC time.

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html

Cisco IOS Release 15.1(1)T2

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T2:

- New CLI introduced to configure polarity detection for 10 Mbps full-duplex links.

Old Behavior: By default, polarity detection is enabled for 10 Mbps full-duplex links on Integrated Services Router Generation 2 (ISR G2) platforms. With connection to some network equipment over a 10 Mbps full-duplex link, the polarity detection feature can cause cyclic redundancy check (CRC) errors. There is no CLI command to disable this feature.

New Behavior: By default, the polarity detection feature is disabled for 10 Mbps full-duplex links on ISR G2 platforms. Use the **rj45-auto-detect-polarity {enable | disable}** command to enable or disable polarity detection.

Additional Information:

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html#wp1067169

- By default, the TCP SIP NAT ALG functionality is disabled.

Old Behavior: In the **ip nat service** command, the **tcp** keyword used along with the **sip** keyword was used to enable the TCP SIP NAT ALG functionality.

New Behavior: The **tcp** keyword used along with the **sip** keyword in the **ip nat service** command is removed. The TCP SIP NAT ALG functionality is disabled by default.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nat.html#wp1049948

Cisco IOS Release 15.1(1)T1

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T1:

- DHCP server sends infinite lease time to the clients.

Old Behavior: DHCP server does not send infinite lease time to the clients for which manual bindings are configured.

New Behavior: DHCP server sends infinite lease time to the clients for which manual bindings are configured.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_svr_cfg.html

- Keyword removed from the **ip nat service** command.

Old Behavior: The **ip nat service** CLI included the **enable-mib** keyword

New Behavior: The **enable-mib** keyword has been deprecated from the **ip nat service** CLI.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nat.html#wp1049948

- The **cns config notify** command is not supported.

Old Behavior: The **cns config notify** command was supported.

New Behavior: The **cns config notify** command will be hidden and not supported effective with Cisco IOS Release 15.1(1)T1.

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_04.html#wp1083435

- Change to BGP path selection.

Old Behavior: BGP selects paths which are not the oldest paths for multipath. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps

New Behavior: BGP uses the best-path selection algorithm to find a set of equally good routes. These routes are the potential multipaths. In Cisco IOS Release 12.2(33)SRD and later releases, when there are more equally good multipaths available than the maximum permitted number, then the oldest paths are selected as multipaths.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_external_sp.html

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_overview.html

- Behavior change for auto-summary (BGP) command.

Old Behavior: When a connected route is automatically summarized by the auto-summary (BGP) command, the route is not deleted from the BGP routing table if the interface assigned that address is shut down.

New Behavior: When a connected route is automatically summarized by the auto-summary (BGP) command, the route is properly deleted from the BGP routing table if the interface assigned that address is shut down.

For more information, see the auto-summary (BGP) command:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp1.html

- Command accounting and command authorization to be sent in asplain notation.

Old Behavior: Command accounting and command authorization that include a 4-byte ASN number are sent in the same format that is used on the command-line interface.

New Behavior: Command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp3.html

http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp4.html

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_10.html

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_11.html

- The **no** form of the **ip nhrp map multicast dyn** command clears all dynamic entries in the multicast table.

Old Behavior: Dynamic entries in the multicast table are not cleared even though the hold time has expired and the **ip nhrp map multicast dyn** command is disabled, which disables the automatic addition of routers to the multicast mappings by NHRP.

New Behavior: All dynamic entries in the multicast table are now cleared when the hold time has expired and the **ip nhrp map multicast dyn** command is disabled.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nhrp.html#wp1011428

- Input error counter is the sum of all error types.

Old Behavior: Each errored packet in the input error counter can report multiple errors, such as CRC, framing, and abort.

New Behavior: Each errored packet in the input error counter reports only one specific error.

Additional Information: The following modules are affected:

WIC-1T,
WIC-2T,
WIC-2A/S,
HWIC-1T,
HWIC-2T,
HWIC-2A/S,
VWIC-xMFT-T1 (or E1),
VWIC2-xMFT-T1/E1,
WIC-1DSU-T1-V2,
HWIC-1DSU-T1,
WIC-1B-U-V2,
WIC-1B-S/T-V3,
HWIC-1B-U (12.4 mainline only),
WIC-xAM,
WIC-xAM-V2

The HWIC and WIC slots in the following platforms are affected:

Cisco 1841
Cisco 2691
Cisco 2801
Cisco 2811, Cisco c2821, Cisco c2851
Cisco 3725, Cisco 3745

- The primary Key Server (KS) now displays a registered Group Encrypted Transport VPN Mode (GM) that is properly encrypting traffic.

Old Behavior: When cooperative key server key distribution occurs, one KS declares itself as the primary KS, creates a policy, and sends out the policy to the other secondary KS. The secondary KS continues to wait before declaring the primary KS as the primary KS and continues to stay in election mode, but since both the primary and secondary KS have a policy, the GM registration succeeds.

New Behavior: When cooperative key server key distribution occurs, one KS declares itself as primary, creates a policy, and sends the policy to the other secondary KS. The secondary KS declares the primary KS as primary KS when it gets the policy and ends the election mode. The secondary KS now also blocks GM registration while the cooperative key server key distribution is in progress. This change allows the cooperative key server distribution to become more efficient because it saves time. For example, the following syslog warning message is displayed:

```
00:00:16: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER_ELECTION: This KS temporarily blocks
GM with ip-addr 10.0.4.1 from registering in group diffint as the KS election is
underway
```

Additional Information: The Cooperative Key Server section in the Cisco Group Encrypted Transport VPN feature document was updated to reflect this change:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

- The auto configuration options are added to the DSL group.

Old Behavior: DSL group did not have auto configuration options. Only manual configuration was allowed.

New Behavior: DSL group provides auto configuration options such as default, exit, no, and shdsl.

Additional Information:

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_d1.html#wp1039345

- The SIP-KPML option is added to the **dtmf-relay** command in voice register pool mode.

Old Behavior: Only three types of audio relay methods were supported in the **dtmf-relay** command under voice register pool.

New Behavior: SIP-KPML option is added as the fourth type of audio relay method in the **dtmf-relay** command under voice register pool in Cisco Unified CME and Cisco Unified SRST.

Additional information:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_d1ht.html#wp1048382

- Error message is displayed when you try applying the tunnel interface to a crypto map.

Old Behavior: Error message is not displayed when you try applying the tunnel interface to a crypto map using the **crypto map** (interface IPsec) command.

New Behavior: An error message is displayed when you try applying the tunnel interface to a crypto map using the **crypto map** (interface IPsec) command.

Additional Information:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#wp1060970

- Right to Use license is added for ISR G2 platforms.

Old Behavior: The Right to Use license is not available for technology packages and all features on Cisco ISR G2 platforms.

New Behavior: The Right to Use license is available for technology packages and all features on Cisco ISR G2 platforms, except for the HSEC feature. Use the license accept end user agreement command in global configuration mode to configure a one-time acceptance of the Cisco End User License Agreement (EULA) for all Cisco IOS software packages and features.

Additional Information:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

Important Notes for Cisco IOS Release 15.1(1)T

This section describes important issue that you should be aware of for Cisco IOS Release 15.1(1)T and later releases.

CISCO-RTTMON-MIB.oid Is Not Supported in the Universal IP Base IOS Technology Package

The Cisco IP Service Letter Agreements (SLAs) responder on a Cisco 2900 series Integrated Service Router (ISR) with the universal ipbasek9 technology package operates as expected. However, any attempt to utilize snmpset or snmpget to retrieve the CiscoRttMonMIB (.1.3.6.1.4.1.9.9.42) module instance identifiers (OIDs) will fail (issuing the **show snmp mib | include rttMonApplResponder** command displays an empty list).

To provide support for snmpset or snmpget and the CISCO-RTTMON-MIB on a Cisco ISR Generation 2 (G2), activate an evaluation license for one of the following technology packages on the Cisco ISR G2: datak9, securityk9, or uck9. Note that evaluation licenses automatically become Right to Use licenses after the initial evaluation period.

Additional Information:

[Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2](#)

Class Calculated Percentage Rate Value

Cisco IOS software ensures that a class's calculated percentage rate value is valid before associating it with an interface.

Old Behavior: When a class with bandwidth, priority, or shape is associated with an interface, Cisco IOS software does not check the class's calculated percentage rate value.

New Behavior: When a class with bandwidth or priority is associated with an interface, Cisco IOS software checks the class's calculated percentage rate value. The value must be between 8 and 2,000,000 kbps. When a class with shape is associated with an interface, Cisco IOS software checks the class's calculated percentage rate value. The value must be between 8,000 and 1,000,000,000 bps. If the values are outside of these ranges, Cisco IOS software does not allow the class to be associated with the interface.

Additional Information:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html#wp1011774

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_n1.html#wp1048842

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_s1.html#wp1060033



Features and Important Notes for Cisco IOS Release 15.1(2)T

Contents

These release notes describe the following topics:

- [New and Changed Information, page 47](#)
- [Important Notes, page 56](#)
- [Limitations and Restrictions, page 62](#)

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1M&T and contains the following subsections:

- [New Hardware Features Supported in Cisco IOS Release 15.1\(2\)T4, page 47](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(2\)T4, page 48](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(2\)T2, page 48](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(2\)T2, page 48](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(2\)T, page 48](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(2\)T, page 50](#)



Note

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at <http://www.cisco.com/go/cfn>.

New Hardware Features Supported in Cisco IOS Release 15.1(2)T4

There are no new hardware features in Cisco IOS Release 15.1(2)T4.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New Software Features Supported in Cisco IOS Release 15.1(2)T4

This section describes new and changed features in Cisco IOS Release 15.1(2)T4. Some features may be new to Cisco IOS Release 15.1(2)T4 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(2)T4. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Right To Use Licensing Support in CLIs and MIBs for Cisco ISR G2 Platforms

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

New Hardware Features Supported in Cisco IOS Release 15.1(2)T2

There are no new hardware features in Cisco IOS Release 15.1(2)T2.

New Software Features Supported in Cisco IOS Release 15.1(2)T2

This section describes new and changed features in Cisco IOS Release 15.1(2)T2. Some features may be new to Cisco IOS Release 15.1(2)T2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(2)T2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

WAAS Express

This feature introduces WAN optimization technology as a software offering on Cisco IOS based platforms. This technology will interoperate with WAN optimization head-end appliances from Cisco.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/cfg_waas_exp.html

New Hardware Features Supported in Cisco IOS Release 15.1(2)T

This section describes new and changed features in Cisco IOS Release 15.1(2)T. Some features may be new to Cisco IOS Release 15.1(2)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(2)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature

does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

1-Port and 2-Port VVIC3s—Voice WAN Interface Cards

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/vd-t1e1_vvic3.html

4-Port and 8-Port Cisco Gigabit EtherSwitch EHWIC Modules for the Integrated Service Routers Generation 2 (ISR G2) Platform

Cisco Gigabit EtherSwitch enhanced high-speed WAN interface cards (EHWICs) are 10/100/1000 BaseT Layer 2 Gigabit Ethernet (GE) switches with an optional power over Ethernet (PoE) module that provides inline power for IP telephones.

Cisco Integrated Service Routers Generation 1 C-Series

Cisco IOS Release 15.1(2)T supports the Cisco 1841C, Cisco 2801C, Cisco 2811C, Cisco 2821C, Cisco 3825C, and Cisco 3845C integrated service routers generation 1 C-series. The following features are not supported on these routers:

- Cisco Communications Manager Express (CME)
- Cisco Unified Border Element (UBE)
- Dynamic Multipoint Virtual Private Network (DMVPN)
- Group Encrypted Transport Virtual Private Network (GET-VPN)
- Hierarchical quality of service (HQoS)
- Multicast features:
 - PIM SSM
 - IGMPv3
 - MVPN
 - MSDP
- NetFlow v9
- Optimized Edge Routing (OER)
- Performance Routing (PFR)
- Power over Ethernet (PoE)
- Survivable Remote Site Telephony (SRST)

Digital Subscriber Line (DSL)—Multimode (VDSL2 and ADSL2/2+)

For detailed information about this feature, see the following documents:

<http://www.cisco.com/en/US/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html>

<http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/hardware/installation/guide/860-880-890HIG.html>

http://www.cisco.com/en/US/docs/ios/bbds1/command/reference/bba_book.html

STM1 Support for Cisco 3900 Series of Platforms

The SM-1-STM1 is a high-speed, single-port multichannel STM-1 port adapter, which serves as a multichannel E1 STM-1 port on Cisco 3900 series integrated services routers (ISR).

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/routers/access/interfaces/adapt/STM1PA/STM1.html>

New Software Features Supported in Cisco IOS Release 15.1(2)T

This section describes new and changed features in Cisco IOS Release 15.1(2)T. Some features may be new to Cisco IOS Release 15.1(2)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(2)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Additional PDL Support for NBAR

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_netwk_traffic.html

Assisted RTCP Packet Generation

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/voice/config_library/12-4t/cube-12-4t-library.html

BFD IPv6 Encapsulation Support

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html>

BGP—Remove/Replace Private AS Filter

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_remove_as_xe.html

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_remove_as.html

BGP Dynamic Neighbors

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html

Bidirectional Forwarding Detection MIB version 2

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd_mib.html

Box to Box (Interchassis) Redundancy for the Cisco Unified Border Element

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html

Cisco CME and SRST Features Enhancement

New features for Cisco Unified CME 8.1:

- Toll Fraud Prevention Enhancement
- Enhancements to SIP Phone Configuration
- Support for Cisco Unified 6901 and 6911 SCCP IP Phones

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmebasic.html

Cisco IOS PKI RA Server Interoperate Support with the Microsoft CA Server

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_mng_cert_serv.html

Cisco IOS ZBFW SCCP Video Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_fwall_skinny_local.html

Cisco IOS Zone-based Firewall

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html

Cisco Unified Border Element—Per-Call Debugging

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html

Cisco Unified Communications Trusted Firewall Control— Version 3

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/TrustedFW.html

DHCP VRF Exclude Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

DMVPN Configuration Using FQDN

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_dmvpn_conf_using_fqdn.html

DMVPN—Tunnel Health Monitoring and Recovery (Backup NHS)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_dmvpn_tun_mon.html

DTLS Support for Cisco IOS SSL VPN

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn.htm

FPM Packaging Feature

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_flex_pack_match.html

Healthcare Router System

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_deploy_RSA_pki.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_mng_cert_serv.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_store_pki_cred.html

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html

IPv6 Support on BVI Interfaces

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html

Layer 2 Switch Port Manageability MIBs for MAC Notification

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html>

MLD Proxy

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html>

MPLS VPN over mGRE

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_mplsvpnmgre.html

OSPFv3 BFD

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html>

Preserve 802.1q with 802.1p Marking over ATM PVCs for xDSL Uplinks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_trans_vlan-tags_dsl_links.html

RSVP for Flexible BW Interface

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html

RSVP over DMVPN

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html

SDP Solution for iPhone Deployment

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_setup_SDP_pi_ki.html

Serviceability Enhancement for PCM Capture

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html

Static Route Support for BFD over IPv6

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html>

Suite-B Support in IOS SW Crypto

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pk_i.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_vpn_ipsec.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_key_exch_ipsec.html

http://www.ciscosystems.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

Support Ability to Configure Source IP Address for Signaling and Media per SIP Trunk

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-bind.html

Support for Call Routing Logic on the Cisco Unified Border Element Based on the Information Embedded in the History-info Header

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Hiding the Internal Topology Information Embedded Within the History-info Header at the Cisco Unified Border Element

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Inclusion of the Authorization Header in the Initial REGISTER Request

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Monitoring Utilization of Critical Resources on Gateway Router, Cisco Unified Border Element and Cisco Unified CME and Reporting Over SIP Trunks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-res_utlzn_monitoring.html

Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-SIP Call on the Cisco Unified Border Element

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_book/vb_book.html

Support for Pass-Through of STUN and DTLS Packets

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/voice/config_library/12-4t/cube-12-4t-library.html

Support for Populating the Route Header Based on the Proxy Server IP Address and Port, and the Service-Route Header Present in the Register Response

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for VMWI over SIP on Cisco IOS Gateways

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-mwi.html

Support Inbound Dial-peer Match Based on the Remote IP Address on SIP Trunks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/gt_url.html

Voice Support on 1-Port and 2-Port HWICs

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_11xw/fmt1e1ic_voice.html

Important Notes

The following information applies to all releases of Cisco IOS Release 15.1T.

- [Cisco IOS Behavior Changes, page 56](#)
- [Important Notes for Cisco IOS Release 15.1\(2\)T, page 61](#)

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- [Cisco IOS Release 15.1\(2\)T5, page 56](#)
- [Cisco IOS Release 15.1\(2\)T4, page 57](#)
- [Cisco IOS Release 15.1\(2\)T3, page 58](#)
- [Cisco IOS Release 15.1\(2\)T2, page 60](#)

Cisco IOS Release 15.1(2)T5

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T5:

- BGP scan time range is changed.
 Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15-60 seconds. The **bgp scan-time** command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).
 New Behavior: The **bgp scan-time** command has a scanner-interval range of 5-60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).
- Change in BGP next-hop for redistributed recursive static routes.
 Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next hop to be itself. The local next-hop (equal to next-hop-self) is kept.
 New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.
- Multicast updates are passed by zone-based firewall with IP multicast traffic.
 Old Behavior: If you use the **drop** (zone-based policy) command to configure a zone-based firewall with IP multicast traffic, all multicast updates are dropped by the zone-based firewall.

New Behavior: All multicast updates are passed by the zone-based firewall even if the zone-based policy configuration includes the **drop** command.

Additional information:

http://cisco.com/en/US/docs/ios-xml/ios/security/d1/dnsix-dmdp_retries_through_dynamic.html#GUID-FC5653D0-8DD9-4ADB-8C03-34A028AEE954

- Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.

Old Behavior: Analog (FXS) phones connected to Cisco IAD2430 are not recognized as SCCP endpoints.

New Behavior: Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.

Additional Information:

<http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fxssccpsplmft.html>

- New keywords “standard” and “system” are added to existing “dtmf-interworking” CLI under voice service and dial-peer configuration modes.

Old Behavior: SIP INFO dtmf digit to RFC4733 DTMF interworking was not supported.

New Behavior: The newly added keyword “standard” generates RTP NTE packets that are RFC 4733 compliant.

Additional information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-d2.html#GUID-ED049ED0-50B0-4C38-B3EE-7DDE625389F4>

- PfR syslog levels are added to minimize number of messages.

Old Behavior: There are too many PfR syslog messages.

New Behavior: PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html>

Cisco IOS Release 15.1(2)T4

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T4:

- BGP no longer activates IPv6 peers in the IPv4 address family automatically.

Old Behavior: By default, both IPv6 and IPv4 capability is exchanged with a BGP peer that has an IPv6 address. When an IPv6 peer is configured, that neighbor is automatically activated under the IPv4 unicast address family.

New Behavior: Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under the IPv4 address family, you can manually deactivate the peer with the **no neighbor ipv6-address activate** command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_basic_net.html

http://www.cisco.com/en/US/partner/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_basic_net_xe_ps11174_TSD_Products_Configuration_Guide_Chapter.html

- A change has been made in the **neighbor prefix-length-size** command.

Old Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, if that neighbor has a peer policy or route map that is removed, the **neighbor prefix-length-size** command setting is also removed.

New Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, the value of that command overrides the value set for the peer-group. If the command is locally configured for the peer, it will not be inherited from the peer-group.

- A change has been made in the **show bgp ipv4 unicast summary** command.

Old Behavior: The **show bgp ipv4 unicast summary** command displays an incorrect number of dynamically created neighbors per address family if a peer-group has been removed from the configuration.

New Behavior: The **show bgp ipv4 unicast summary** command displays the correct number of dynamically created neighbors, even if a peer-group has been removed. The output displays the number of dynamically created neighbors per address family, and at the end of output, displays the total number of dynamically created neighbors on the router.

- The **ntp panic update** command is introduced.

Old Behavior: There is no command to configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds.

New Behavior: A new command, **ntp panic update**, is introduced to configure NTP to reject time updates greater than the panic threshold of 1000 seconds. If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

```
NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000.
seconds; set clock manually to the correct UTC time.
```

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html

- A CERM license is reserved only after the user logs in.

Old Behavior: A Crypto Export Restrictions Manager (CERM) license is reserved for every SSL or Transport Layer Security (TLS) session.

New Behavior: A CERM license is reserved only after the user logs in.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-1mt/sec-conn-ssl-vpn-ssl-vpn.html

Cisco IOS Release 15.1(2)T3

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T3:

- By default, the TCP SIP NAT ALG functionality is disabled.

Old Behavior: In the **ip nat service** command, the **tcp** keyword used along with the **sip** keyword was used to enable the TCP SIP NAT ALG functionality.

New Behavior: The **tcp** keyword used along with the **sip** keyword in the **ip nat service** command is removed. The TCP SIP NAT ALG functionality is disabled by default.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nat.html#wp1049948

- The **show ip multicast rpf tracked** command is no longer supported.

Old Behavior: The **show ip multicast rpf tracked** command is available for use. However, it is not recommended that customers use this command.

New Behavior: The **show ip multicast rpf tracked** command is removed.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_06.html

- Default maximum is removed for subinterface queue-limit.

Old Behavior: The default maximum queue-limit on a subinterface was 512 if no hold-queue was configured on the main interface.

New Behavior: As part of HQF, this restriction has been removed. Now the maximum queue-limit can be set as high as the hold-queue size on the main interface.

Additional Information:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_q1.html#wp1075320

- BGP address families no longer stuck in NoNeg or idle state after reload

Old Behavior: After a reload of a router, some or all of the BGP address families do not come up. This is because the router is receiving messages from a neighbor that the AFI or SAFI is not supported, and the router does not retry those AFIs. The output of show ip bgp all summary shows the address family in NoNeg or idle state, and it will never leave that state. Typical output looks like:

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
x.x.x.x 4 1 0 0 1 0 0 never (NoNeg)
```

New Behavior: When the router receives a message that the AFI or SAFI is not supported, the router does not simply drop the rejected AFIs or SAFIs from subsequent OPEN messages. Instead, the router retries the AFI/SAFI within the existing OPEN message retry timing sequence, but with an exponential backoff (stopping at 10 minutes) applied to decisions about whether to include a particular AFI/SAFI in an OPEN message. The timing of OPEN messages is not changed. Successful negotiation of the AFI results in a reset of the backoff sequence for future attempts. Also, when a BGP connection collision occurs with a session in the ESTABLISHED state, BGP sends a CEASE notification on the newly opened connection, and a keepalive message on the old connection. The new connection is closed. If the old session was stale, the keepalive causes it to be closed. The neighbor will retry its OPEN message after receiving the CEASE message and waiting a few seconds.

- New BGP Error Message

Old Behavior: No error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels (via the neighbor send-label command or via a template). Sending MPLS labels to IPv6 peers is not supported.

New Behavior: An error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels. An example of the error message is
 “%BGP-4-BGP_LABELS_NOT_SUPPORTED: BGP neighbor 2001:DB8:1::2 does not support sending labels.”

- The summary address is not advertised to the peer.

Old Behavior: The summary address is advertised to the peer if the administrative distance is configured as 255.

New Behavior: The summary address is not advertised to the peer if the administrative distance is configured as 255.

- Two new keywords, **protocol** and **pbr**, are added to the **mode route** command.

Old Behavior: Destination-only traffic classes cannot be controlled when more than one protocol is operating at the border routers.

New Behavior: Destination-only traffic classes can be controlled when more than one protocol is operating at the border routers using dynamic PBR.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html>

- On Cisco 860, 880, 890, 2900, and 3900 series ISRs, the default behavior changes when the interface is not connected to an active port:

Old Behavior: GigabitEthernet0/3/0 is up, line protocol is down.

New Behavior: GigabitEthernet0/3/0 is down, line protocol is down.

- The line coding and loss of sync information is changed in the output for the **show controller shdsl** command.

Old Behavior: The output for the **show controller shdsl** command for the HWIC- 4SHDSL-E shows the line coding as AUTO-TCPAM when Annex F and G are selected, and loss of sync as LOSWAS.

New Behavior: The output for the **show controller shdsl** command for the HWIC- 4SHDSL-E shows the line coding as 16-TCPAM or 32-TCPAM depending on which TCPAM is used to train lines when Annex F and G are selected, and loss of sync as LOSW.

Additional Information:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_HWICS.html

- Behavior change type: New keyword added to **ignore crc** command.

Old Behavior: The **always** keyword was not available for the **ignore crc** command.

New Behavior: The **ignore crc** command can use the **always** keyword to always ignore CRC errors.

Additional information:

http://www.cisco.com/en/US/docs/ios/bbds/command/reference/bba_book.html

Cisco IOS Release 15.1(2)T2

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T2:

- Specific BGP **show** commands display dampening information on an individual VRF basis.

Old Behavior: The following commands display flap-statistics, dampened-paths, and dampening parameters of VRFs under the VPNv4 or VPNv6 address family identifier:

- **show ip bgp all dampening**
- **show ip bgp vpnv4 all dampening**
- **show ip bgp vpnv6 unicast all dampening**

New Behavior: Because VRFs can have dampening enabled independently of other VRFs and the global VPNv4 and VPNv6 topologies, the following commands display flap-statistics, dampened-paths, and dampening parameters of individual VRFs under that VRF name:

- **show ip bgp all dampening**
- **show ip bgp vpnv4 all dampening**
- **show ip bgp vpnv6 unicast all dampening**

If dampening is not enabled for a VRF, that is stated under the VRF name.

For more information, see the [Cisco IOS IP Routing: BGP Command Reference](#).

- Command is changed to disable pipelining for URLF requests to Trend Server.
 Old Behavior: Trend Router Provisioning Server (TRPS) does not provide the functionality to turn on or off the TRPS pipeline requests.
 New Behavior: TRPS enables you to turn on or off the TRPS pipeline requests.
 The **pipeline**, **on**, and **off** keywords are added to the **parameter-map type trend-global** command.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_p1.html#wp1059633
- New command is introduced to configure polarity detection for 10-Mbps full-duplex links.
 Old Behavior: By default, polarity detection is enabled for 10-Mbps full-duplex links on Integrated Services Router Generation 2 (ISR G2) platforms. With connection to some network equipment over a 10-Mbps full-duplex link, the polarity detection feature can cause cyclic redundancy check (CRC) errors. There is no CLI command to disable this feature.
 New Behavior: By default, the polarity detection feature is disabled for 10-Mbps full-duplex links on ISR G2 platforms. Use the **rj45-auto-detect-polarity {enable | disable}** command to enable or disable polarity detection.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html#wp1067169
- The default state for the Cisco Gigabit EtherSwitch EHWIC when the interface is not connected to an active port is changed.
 Old Behavior: GigabitEthernet0/3/0 is up, line protocol is down.
 New Behavior: GigabitEthernet0/3/0 is down, line protocol is down.
- Right to Use license is added for ISR G2 platforms.
 Old Behavior: The Right to Use license is not available for technology packages and all features on Cisco ISR G2 platforms.
 New Behavior: The Right to Use license is available for technology packages and all features on Cisco ISR G2 platforms, except for the HSEC feature. Use the license accept end user agreement command in global configuration mode to configure a one-time acceptance of the Cisco End User License Agreement (EULA) for all Cisco IOS software packages and features.
 Additional Information:
http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

Important Notes for Cisco IOS Release 15.1(2)T

The following information applies to all releases of Cisco IOS Release 15.1(2)T:

Images Deferred Because of Caveat CSCti18193

In Cisco IOS Release 15.1(2)T, images for all platforms have been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCti18193. With caveat CSCti18193, Cisco IOS Release 15.1(2)T is affected by denial of service (DoS) vulnerability during TCP establishment phase. The software solution for these deferred images is Cisco IOS Release 15.1(2)T0a.



Note

Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Toll Fraud Prevention

In Cisco IOS Release 15.1(2)T, the Toll Fraud Prevention feature is supported as below:

- Source IP address authentication is enabled on incoming IPv4 H323/ or SIP trunk calls. The source IP address of any incoming IPv4 H323 or SIP trunk calls will be authenticated based on:
 - Manually configured IP address trusted list.
 - VoIP dial-peer session target (the state of a VoIP dial-peer must be in “Operation State = UP”)

Incoming IPv4 H323 or SIP trunk calls will be rejected if the authentication fails and the default **cause-code call-reject (21)** disconnects the call.

Execute the **show ip address trusted list** command to display IP address trusted data and a list of valid source IP addresses. The default behavior can be disabled as shown in the example below:

```
voice service voip
no ip address trusted authenticate
```

- Secondary dial-tone is disabled for a call initiated from a FXO port. No secondary dial-tone causes the outgoing call setup to fail if the called number is NULL. The default behavior can be disabled as shown below:

```
voice-port <fxo-port>
secondary dialtone
```

- Direct-inward-dial is enabled to prevent the toll fraud for incoming ISDN calls. Two-stage dialing is disabled for incoming ISDN calls by default. The incoming called number will then be used for outgoing call setup. The default behavior can be disabled as shown in the example below:

```
voice service pots
no direct-inward-dial isdn
```

For more information, see the *Cisco Unified Communications Manager Express System Administrator Guide* at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Limitations and Restrictions

Any limitations and restrictions that apply to Cisco IOS Release 15.1M&T will be documented here.

Limitations and Restrictions in Cisco IOS Release 15.1(2)T2a

This section describes limitations and restrictions in Cisco IOS Release 15.1(2)T2a and later releases.

FIPS Certification

Cisco IOS Release 15.1(2)T2a is only to provide FIPS certification for the Cisco ISR Generation 2 platforms.



Features and Important Notes for Cisco IOS Release 15.1(3)T

Contents

These release notes describe the following topics:

- [New and Changed Information, page 65](#)
- [Important Notes, page 73](#)

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1M&T and contains the following subsections:

- [New Hardware Features Supported in Cisco IOS Release 15.1\(3\)T4, page 65](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(3\)T4, page 66](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(3\)T2, page 66](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(3\)T2, page 66](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(3\)T, page 66](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(3\)T, page 67](#)



Note

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at <http://www.cisco.com/go/cfn>.

New Hardware Features Supported in Cisco IOS Release 15.1(3)T4

There are no new hardware features in Cisco IOS Release 15.1(3)T4.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

New Software Features Supported in Cisco IOS Release 15.1(3)T4

There are no new software features in Cisco IOS Release 15.1(3)T4.

New Hardware Features Supported in Cisco IOS Release 15.1(3)T2

There are no new hardware features in Cisco IOS Release 15.1(3)T2.

New Software Features Supported in Cisco IOS Release 15.1(3)T2

This section describes new and changed features in Cisco IOS Release 15.1(3)T2. Some features may be new to Cisco IOS Release 15.1(3)T2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Right To Use Licensing Support in CLIs and MIBs for Cisco ISR G2 Platforms

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

New Hardware Features Supported in Cisco IOS Release 15.1(3)T

This section describes new and changed features in Cisco IOS Release 15.1(3)T. Some features may be new to Cisco IOS Release 15.1(3)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

EHWIC Multimode VDSL2/ADSL+

The EHWIC-VA-DSL-A, EHWIC-VA-DSL-B, and EHWIC-VA-DSL-M are Multi-mode VDSL/ADSL2+ HWICs.

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/bbdsi/command/reference/bba_02.html#wp1048705

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/dsl_hwic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/inst_ic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/oview_ic.html

<http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html>

VDSL HWIC: HWIC-1VDSL over POTS

The HWIC-1VDSL is used on the Cisco 3945E ISR and the Cisco 3925E ISR to provide VDSL over POTS WAN connectivity. It can be installed on Cisco ISR G2 platforms, and the external RJ-11 port is connected to a DSL line coming from VDSL2 supported DSLAM.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/vdsl2_hwic.html

VWIC3—4MFT-T1/E1

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/customer/docs/routers/access/interfaces/software/feature/guide/vd-t1e1_4p_vwic3.html

New Software Features Supported in Cisco IOS Release 15.1(3)T

This section describes new and changed features in Cisco IOS Release 15.1(3)T. Some features may be new to Cisco IOS Release 15.1(3)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Advanced FXS Analog Gateway Features and SCCP over TLS with Cisco UCM

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/15_1/fxs_15_1_cg_book.html

Cisco CME and SRST Features Enhancement for SCCP and SIP

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Cisco IOS PKI Performance Monitoring Enhancements

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_deploy_RSA_pki.html

Cisco IOS SSL VPN Smart Tunnels Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/partner/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn_smart_tunnels_support.html

Cisco ISR G2 Multi Gigabit Fabric

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/mgfcfg.html>

DHCP—Tunnels Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_dmvpn_dhcp_tunnels_support.html

Embedded Event Manager 3.2

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html

Enhancement to Bandwidth QoS-Reference Command

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html

GETVPN Troubleshooting

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

IKEv1 Hardening

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_call_addmsn_ike.html

IKEv2 Remote Access Headend

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

IP Tunneling—IPv6 Rapid Deployment

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html>

IPv6—Full Selective Packet Discard Support

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-spd.html>

IPv6—Per Interface Neighbor Discovery Cache Limit

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html

ISDN Leased Line

The ISDN Leased Line Support for C880 Platforms feature allows the user to configure a dial-up interface to obtain a leased line, which is virtually a permanent connection. After an ISDN BRI interface is configured for access over leased lines, it is no longer a dialer interface, and signaling over the D channel no longer applies.

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/routers/access/800/software/release/notes/rn880isdn.html>

Legacy QoS Command Deprecation: Hidden Commands

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/legacy_qos_cli_deprecation_xe.html

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/legacy_qos_cli_deprecation.html

MediaTrace 1.0

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_mediatrace.htm

Multicast for Virtual Multipoint Interfaces

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/ipmobility/configuration/guide/imo_adhoc_rtr2rd.html

http://www.cisco.com/en/US/products/ps5845/products_installation_and_configuration_guides_list.html

NBAR Static IPv4 IANA Protocols

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar.html

NSE Capability Negotiations via SDP

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/mgcp/configuration/guide/vm_mgcp_basic_cfg.html

Performance Monitor (Phase 1)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_pasv_mon.html

Radio Aware Routing RFC 4938bis

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipmobility/configuration/guide/imo_adhoc_rtr2rd.html

RSVP Support for Ingress Call Admission Control

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html

Session-Based FPM

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_flex_pack_match.html

Suite-B IPSec Algorithm Support for the On-Board Crypto Engine for Cisco 2951 and Cisco 3900 Series ISRs

The Suite-B IPSec algorithm in the hardware crypto engine is now supported on the Cisco 2951 and 3900 Series Integrated Services Router platforms. Suite-B requirements comprise four user-interface suites of cryptographic algorithms for use with IKE and IPSec that are described in RFC 4869. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm.

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pk_i.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_vpn_ipsec.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_key_exch_ipsec.html

http://www.ciscosystems.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

Support for Conditional Header Manipulation of SIP Headers

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html>

Support for Interworking Between CUCM-Controlled RSVP-Capable Networks and RSVP-Incapable Networks

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-h323sip.html>

Support for Limiting the Rate of Incoming SIP Calls Processing

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-roadmap.html>

Support for Media Flow-Around with SIP Signaling Control on Cisco UBE

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-h323h323.html#wp1318874>

Support for Release of Media Flow with Retention of SIP Signaling Control on Cisco UBE for Media Trombone or Media Hairpin Call Is Detected

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-h323h323.html>

Support for Reporting End-of-Call Statistics in SIP BYE Message

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html>

Support for SIP Registration Proxy on Cisco UBE

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html>

Support for SIP UPDATE Message per RFC 3311

For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html>

Switch Image and Configuration Manageability

Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. This release supports a new MIB, CISCO-SMART-INSTALL-MIB.my. For information about the new features and the MIB, see the *Smart Install Configuration Guide, Release 12.2(55)SE* at the following URL:

http://cisco.com/en/US/docs/switches/lan/smart_install/release_12.2_55_se/configuration/guide/smart_install3.html

Video Monitoring MIB Support for Medianet Video Monitoring

This feature provides support for the use of the industry-standard Simple Network Management Protocol (SNMP) to monitor media streams. This support is implemented with the addition of the following Cisco proprietary SNMP Management Information Base (MIB) modules:

- **CISCO-FLOW-MONITOR-TC-MIB**—Defines the textual conventions common to the following MIB modules.
- **CISCO-FLOW-MONITOR-MIB**—Defines the framework that describes the flow monitors supported by a system, the flows that it has learned, and the flow metrics collected for those flows.
- **CISCO-RTP-METRICS-MIB**—Defines objects that describe the quality metrics collected for RTP streams, similar to those described by an RTCP Receiver Report packet [RFC 3550].
- **CISCO-IP-CBR-METRICS-MIB**—Defines objects that describe the quality metrics collected for IP streams that have a Constant Bit Rate (CBR).

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at <http://www.cisco.com/go/mibs>.

This feature also includes two new command-line interface (CLI) commands and one modified CLI command. The commands are as follows:

- **snmp-server host**—Enables the delivery of flow monitoring SNMP notifications to a recipient.
- **snmp-server enable traps flowmon**—Enables flow monitoring SNMP notifications. By default, flow monitoring SNMP notifications are disabled.
- **snmp mib flowmon alarm history**—Sets the maximum number of entries maintained by the flow monitor alarm history log.

For more information about these commands, see the *Cisco IOS Master Command List*.

Important Notes

The following information applies to all releases of Cisco IOS Release 15.1T.

- [Cisco IOS Behavior Changes, page 73](#)

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- [Cisco IOS Release 15.1\(3\)T4, page 73](#)
- [Cisco IOS Release 15.1\(3\)T3, page 74](#)
- [Cisco IOS Release 15.1\(3\)T2, page 75](#)
- [Cisco IOS Release 15.1\(3\)T1, page 76](#)

Cisco IOS Release 15.1(3)T4

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T4:

- SIP call hold/resume scenario has been enhanced so that the RTP sequence number is continuous from the origin of the call till the end.

Old Behavior: The RTP sequence number is not continuous from the origin until the end of a SIP call, including the time when the call is on hold.

New Behavior: The RTP sequence number is now continuous from the origin until the end of a SIP call.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-1mt/sip-to-sip_supplementary_services_for_session_border_controller.html

- The new keywords **standard** and **system** are added to the existing **dtmf-interworking** CLI under voice service and dial-peer configuration modes.

Old Behavior: SIP INFO dtmf digit to RFC4733 DTMF interworking was not supported.

New Behavior: The newly added keyword **standard** generates RTP NTE packets that are RFC 4733-compliant.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-d2.html#GUID-ED049ED0-50B0-4C38-B3EE-7DDE625389F4>

- PfR syslog levels are added to minimize number of messages.

Old Behavior: There are too many PfR syslog messages.

New Behavior: PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html>

Cisco IOS Release 15.1(3)T3

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T3:

- The lease time for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
Old Behavior: DHCP server was sending infinite lease time to manual binding clients.
New Behavior: The DHCP server sends a finite lease (the value configured using the **lease** command in DHCP pool configuration mode) to the clients for which manual bindings are configured.
- New keywords are added to the **ip access-list** command.
Old Behavior: There is no filtering capability on packets with IP helper-address destinations.
New Behavior: Filtering capability is supported for packets with IP helper-address destinations.
Additional Information:
http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_11.html
- The **all** keyword was added to the **ipv6 nd ra suppress** command.
Old Behavior: The **all** keyword was not part of command syntax.
New Behavior: Use of the **all** keyword with the **ipv6 nd ra suppress** command suppresses all IPv6 router advertisements, periodic multicast and solicited, on an interface.
Additional Information:
<http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-i3.html#GUID-1C8D6870-C7DC-4C4B-A6F1-00FA21506E1E>
- BGP scan time range is changed.
Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15 to 60 seconds. The **bgp scan-time** command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).
New Behavior: The **bgp scan-time** command has a scanner-interval range of 5 to 60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).
- An ADSL interface fails to retrain when the **dsl enable-training-log** command is configured.
Old Behavior: When the **dsl enable-training-log** command is configured and a cable is disconnected from an asymmetric digital subscriber line (ADSL) card and then reconnected, the ADSL interface fails to retrain.
New Behavior: To prevent this from happening, disable the retrieval of the DSL training log using the **no dsl enable-training-log** command. The DSL will now train up to the DSLAM.
Additional Information:
<http://www.cisco.com/en/US/docs/ios-xml/ios/bbds/command/bba-a1.html>
- Change in BGP next-hop for redistributed recursive static routes.
Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next hop to be itself. The local next-hop (equal to next-hop-self) is kept.
New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.

Cisco IOS Release 15.1(3)T2

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T2:

- BGP no longer activates IPv6 peers in the IPv4 address family automatically.

Old Behavior: By default, both IPv6 and IPv4 capability is exchanged with a BGP peer that has an IPv6 address. When an IPv6 peer is configured, that neighbor is automatically activated under the IPv4 unicast address family.

New Behavior: Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under the IPv4 address family, you can manually deactivate the peer with the **no neighbor ipv6-address activate** command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_basic_net.html

http://www.cisco.com/en/US/partner/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_basic_net_xe_ps11174_TSD_Products_Configuration_Guide_Chapter.html

- A change has been made in the **neighbor prefix-length-size** command.

Old Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, if that neighbor has a peer policy or route map that is removed, the **neighbor prefix-length-size** command setting is also removed.

New Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, the value of that command overrides the value set for the peer-group. If the command is locally configured for the peer, it will not be inherited from the peer-group.

- A change has been made in the **show bgp ipv4 unicast summary** command.

Old Behavior: The **show bgp ipv4 unicast summary** command displays an incorrect number of dynamically created neighbors per address family if a peer-group has been removed from the configuration.

New Behavior: The **show bgp ipv4 unicast summary** command displays the correct number of dynamically created neighbors, even if a peer-group has been removed. The output displays the number of dynamically created neighbors per address family, and at the end of the output, displays the total number of dynamically created neighbors on the router.

- If there is cause for an IKE registration security association to be deleted on a GDOI group member, it will also be deleted for all groups that share it.

Old Behavior: When an IKE registration SA is shared among multiple GDOI groups, it is not consistently cleared on members of all groups.

New Behavior: If there is cause for an IKE registration SA to be deleted on a group member (even if another group is still running and has previously registered through it), it will be deleted for all groups.

Additional Information:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

- The hold-alert notification period is not adjustable after first timeout.

Old Behavior: The hold-alert notification period is not adjustable after first timeout.

New Behavior: The hold-alert notification period is adjustable after first timeout. The recurrence <recurrence-timeout> parameter has been added.

Additional Information:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_h1ht.html#wp1021169

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmering.html#wp1013688

- A CERM license is reserved only after the user logs in.

Old Behavior: A Crypto Export Restrictions Manager (CERM) license is reserved for every SSL or Transport Layer Security (TLS) session.

New Behavior: A CERM license is reserved only after the user logs in.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-1mt/sec-conn-ssl-vpn-ssl-vpn.html

- Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.

Old Behavior: Analog (FXS) phones connected to Cisco IAD2430 are not recognized as SCCP endpoints.

New Behavior: Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.

Additional Information:

<http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fxscccpsplmft.html>

- The **ntp panic update** command is introduced.

Old Behavior: There is no command to configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds.

New Behavior: A new command, **ntp panic update**, is introduced to configure NTP to reject time updates greater than the panic threshold of 1000 seconds. If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

```
NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000.
seconds; set clock manually to the correct UTC time.
```

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html

- The **cable-detect** command does not support analog FXO ground-start voice port.

Old Behavior: The **cable-detect** command can be configured on analog FXO loop-start, ground-start, and cama voice port.

New Behavior: The **cable-detect** command cannot be configured on analog FXO ground-start voice port. This command is supported only for analog FXO loop-start and cama voice port.

Cisco IOS Release 15.1(3)T1

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T1:

- The **show ip multicast rpf tracked** command is no longer supported.

Old Behavior: The **show ip multicast rpf tracked** command is available for use. However, it is not recommended that customers use this command.

New Behavior: The **show ip multicast rpf tracked** command is removed.

Additional Information:\

http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_06.html

- Default maximum removed for subinterface queue-limit.

Old Behavior: The default maximum queue-limit on a subinterface is 512 if no hold-queue is configured on the main interface.

New Behavior: As part of HQF, this restriction has been removed. Now, the maximum queue-limit can be set as high as the hold-queue size on the main interface.

Additional Information:

http://www.cisco.com/en/US/partner/docs/ios/qos/command/reference/qos_q1.html#wp1075320

- Input service policies are not implemented for PPPoE client traffic.

Old Behavior: Input service policies attached to a main interface or a subinterface are not implemented for PPPoE client traffic. Only input service policies attached to a dialer interface are implemented.

New Behavior: Input service policies attached to a main interface or a subinterface are implemented for PPPoE client traffic but only if an input service policy is not configured for a dialer interface. If an input service policy is configured for a dialer interface, the old behavior is retained. Only the quality of service (QoS) counters for packet classification are supported. Counters for packet dropping, packet marking, and policing actions are not supported and are ignored.

- BGP address families are no longer stuck in NoNeg or idle state after reload.

Old Behavior: After a reload of a router, some or all of the BGP address families do not come up. This is because the router is receiving messages from a neighbor that the AFI or SAFI is not supported, and the router does not retry those AFIs. The output of **show ip bgp all summary** command shows the address family in NoNeg or idle state, and it will never leave that state. Typical output looks like:

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
x.x.x.x 4 1 0 0 1 0 0 never (NoNeg)
```

New Behavior: When the router receives a message that the AFI or SAFI is not supported, the router does not simply drop the rejected AFIs or SAFIs from subsequent OPEN messages. Instead, the router retries the AFI/SAFI within the existing OPEN message retry timing sequence, but with an exponential back off (stopping at 10 minutes) applied to decisions about whether to include a particular AFI/SAFI in an OPEN message. The timing of OPEN messages is not changed. Successful negotiation of the AFI results in a reset of the backoff sequence for future attempts. Also, when a BGP connection collision occurs with a session in the ESTABLISHED state, BGP sends a CEASE notification on the newly opened connection, and a keepalive message on the old connection. The new connection is closed. If the old session is stale, the keepalive causes it to be closed. The neighbor will retry its OPEN message after receiving the CEASE message and waiting a few seconds.

- New BGP error message

Old Behavior: No error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels (via the **neighbor send-label** command or via a template). Sending MPLS labels to IPv6 peers is not supported.

New Behavior: An error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels. An example of the error message is as follows:

```
%BGP-4-BGP_LABELS_NOT_SUPPORTED: BGP neighbor 2001:DB8:1::2 does not support sending labels.
```

- The summary address is not advertised to the peer.
 Old Behavior: The summary address is advertised to the peer if the administrative distance is configured as 255.
 New Behavior: The summary address is not advertised to the peer if the administrative distance is configured as 255.
- Two new keywords, **protocol** and **pbr**, are added to the **mode route** command.
 Old Behavior: Destination-only traffic classes cannot be controlled when more than one protocol is operating at the border routers.
 New Behavior: Destination-only traffic classes can be controlled when more than one protocol is operating at the border routers using dynamic PBR.
 Additional Information:
<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html>
- On the Cisco 860, 880, 890, 2900, and 3900 series ISRs, the default behavior changes when the interface is not connected to an active port.
 Old Behavior: GigabitEthernet0/3/0 is up, line protocol is down.
 New Behavior: GigabitEthernet0/3/0 is down, line protocol is down.
- A new keyword is added to the **ignore crc** command.
 Old Behavior: The **always** keyword is not available for the **ignore crc** command.
 New Behavior: The **ignore crc** command can use the **always** keyword to always ignore CRC errors.
 Additional information:
http://www.cisco.com/en/US/docs/ios/bbdsi/command/reference/bba_book.html
- A new keyword is added to the **bind interface** command
 Old Behavior: The **dynamic** keyword is not available for the **bind interface** command.
 New Behavior: The **bind interface** command can use the **dynamic** keyword.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_b1.html#wp1545540



Features and Important Notes for Cisco IOS Release 15.1(4)M

Contents

These release notes describe the following topics:

- [New and Changed Information, page 79](#)
- [Important Notes, page 89](#)

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1(4)M and contains the following subsections:

- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M7, page 80](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M7, page 80](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M6, page 80](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M6, page 80](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M5, page 80](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M5, page 80](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M4, page 80](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M4, page 81](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M3, page 81](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M3, page 81](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M2, page 81](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M2, page 82](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M2, page 81](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M2, page 82](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M1](#), page 82
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M1](#), page 83
- [New Hardware Features Supported in Cisco IOS Release 15.1\(4\)M](#), page 83
- [New Software Features Supported in Cisco IOS Release 15.1\(4\)M](#), page 85

**Note**

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at <http://www.cisco.com/go/cfn>.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M7

There are no new hardware features in Cisco IOS Release 15.1(4)M7.

New Software Features Supported in Cisco IOS Release 15.1(4)M7

There are no new software features in Cisco IOS Release 15.1(4)M7.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M6

There are no new hardware features in Cisco IOS Release 15.1(4)M6.

New Software Features Supported in Cisco IOS Release 15.1(4)M6

There are no new software features in Cisco IOS Release 15.1(4)M6.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M5

There are no new hardware features in Cisco IOS Release 15.1(4)M5.

New Software Features Supported in Cisco IOS Release 15.1(4)M5

There are no new software features in Cisco IOS Release 15.1(4)M5.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M4

This section describes new and changed features in Cisco IOS Release 15.1(4)M4. Some features may be new to Cisco IOS Release 15.1(4)M4 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(4)M4. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Cisco Connected Grid 2G/3G/4G LTE GRWIC for Verizon Wireless

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/connectedgrid/modules/4g/install/CG_2G-3G-4G_Multimode_LTE_GRWIC.html

New Software Features Supported in Cisco IOS Release 15.1(4)M4

There are no new software features in Cisco IOS Release 15.1(4)M4.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M3

There are no new hardware features in Cisco IOS Release 15.1(4)M3.

New Software Features Supported in Cisco IOS Release 15.1(4)M3

There are no new hardware features in Cisco IOS Release 15.1(4)M3.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M2

This section describes new and changed features in Cisco IOS Release 15.1(3)T32. Some features may be new to Cisco IOS Release 15.1(3)T32 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T32. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Cisco 860 Series Integrated Services Routers

The Cisco 860 series integrated services routers (ISRs) combine Internet access, security, and wireless services onto a single, secure device that is simple to use and manage for small businesses. Cisco 860 ISRs are fixed-configuration routers that provide business solutions for secure voice and data communication to small businesses. The Cisco 860 series offers secure broadband services over Gigabit Ethernet and DSL Multi-mode (VDSL2 / ADSL2/2+) WAN links.

Cisco 881-V, Cisco 887VA-V, and Cisco 887VA-V-W

The Cisco 881-V, Cisco 887VA-V, and Cisco 887VA-V-W integrated services routers deliver analog and digital voice support as well as data. For more information on the product, see the following documentation:

<http://www.cisco.com/en/US/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html>

<http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/hardware/installation/guide/860-880-890HIG.html>

SM-32A Module Support on Cisco 3900/3900E Integrated Services Routers G2 Platforms

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/sm_32a.html

New Software Features Supported in Cisco IOS Release 15.1(4)M2

There are no new software features in Cisco IOS Release 15.1(4)M2.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M1

This section describes new and changed features in Cisco IOS Release 15.1(3)T31. Some features may be new to Cisco IOS Release 15.1(3)T31 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T31. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

3G Cisco IOS Fixed Router

The Cisco 819G and Cisco 819GH integrated services router (ISR) is a compact 3G Cisco IOS fixed router that can operate in outdoor, indoor, and mobile environments. The Cisco 819 ISRs are available in hardened and non-hardened versions. The Cisco 819GH ISR is the hardened version that operates over an extended temperature range. The Cisco 819G ISR is a standard form factor with a commercial operating range. The Cisco 819 integrated services routers support the latest 3G speeds (High-Speed Packet Access Plus [HSPA+] and Evolution Data Optimized [EVDO Rev A]), enabling up to 4G speeds. They are backward-compatible with High-Speed Packet Access (HSPA), Universal Mobile Telecommunications Service (UMTS), Enhanced Data Rates for Global Evolution (EDGE), General Packet Radio Service (GPRS), and EVDO Rev 0/1xRTT. It can also be used as a primary WAN data link. The 3G technology is third-generation wide-area cellular technology that is used in voice telephony and broadband wireless data in a mobile environment.

The Cisco 819 ISR is a desktop form factor with built-in wall-mount features and optional rack-mount features. These routers are powered by an external AC power supply adapter.

For detailed information about this feature, see the following hardware document:

<http://cisco.com/en/US/docs/routers/access/800/819/hardware/install/guide/819hwinst.html>

For detailed information about this feature, see the following software document:

http://www.cisco.com/en/US/docs/routers/access/800/819/software/configuration/Guide/819_SCG.html

New Software Features Supported in Cisco IOS Release 15.1(4)M1

This section describes new and changed features in Cisco IOS Release 15.1(3)T31. Some features may be new to Cisco IOS Release 15.1(3)T31 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T31. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed is available in the feature description provided.

Right To Use Licensing Support in CLIs and MIBs for Cisco ISR G2 Platforms

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

New Hardware Features Supported in Cisco IOS Release 15.1(4)M

This section describes new and changed features in Cisco IOS Release 15.1(3)T3. Some features may be new to Cisco IOS Release 15.1(3)T3 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T3. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

China VWIC2-1MFT-G703-C and VWIC2-2MFT-G703-C Modules Support onto Cisco 1906C/K9 Supported Module List

The Cisco 1906C was built on the Cisco 1900 Series Integrated Services Routers (ISRs) based on first-class products. All Cisco 1900 Series ISR products offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and advanced security services. In addition, the Cisco 1906C ISR has an integrated serial interface module and an EWHIC slot that can support LAN, 3G, or ISDN module options. It can be deployed in a high-speed WAN environment, which provides better service integration capabilities and network flexibility. The Cisco 1906C improves performance and density and will support multiple services. It will also feature multiple independent devices that can be integrated into a compact remote management system. The Cisco second-generation 1- and 2-port T1/E1 Multiflex Trunk Voice/WAN Interface cards (MFT VWIC2s) support data on the Cisco 1906C Series ISRs. The Cisco MFT VWIC2 combines WAN-interface-card (WIC) and voice-interface-card (VIC) functions to provide unparalleled flexibility, versatility, and investment protection through its many uses.

For more information, see the following document:

http://www.cisco.com/en/US/docs/routers/access/1900/hardware/release/notes/Rn_C1906K9.html

Cisco Gigabit Ethernet/SFP Enhanced High-Speed WAN Interface Card

The Cisco Gigabit Ethernet WAN EHWIC (EHWIC-1GE-SFP-CU) is an enhanced high-speed interface card providing copper and optical Gigabit Ethernet ports and connectivity of T1/E1 and T3/E3 over copper for Cisco Integrated Services Routers (ISRs). The Cisco Gigabit Ethernet enhanced high-speed WAN interface card also provides copper and optical Gigabit Ethernet connectivity through a dual-purpose uplink (DPU).

Cisco ISR VE Series

Cisco IOS Release 15.1(4)M supports the Cisco 1841VE and Cisco 2811VE Integrated Services Routers (ISRs). The Cisco 1841VE router offer the following features:

- Embedded hardware-based encryption enabled by an optional Cisco IOS software security image
- Further enhancement of VPN performance with an optional VPN acceleration module
- Firewall functions
- Interfaces for a wide range of connectivity requirements, including support for optional integrated switch ports
- Sufficient performance and slot density for future network expansion and advanced applications
- An integrated real-time clock

The Cisco 2811VE features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1 connections. The routers offer the following features:

- Embedded encryption acceleration and on-the-motherboard voice Digital Signal Processor (DSP) slots
- Intrusion prevention system (IPS) and firewall functions
- High-density interfaces for a wide range of wired and wireless connectivity requirements
- Sufficient performance and slot density for future network expansion requirements and advanced applications

EHWIC Multi-Mode VDSL2/ADSL+ Multicard Support

The HWIC-ADSL-VDSL2 offers multi-mode VDSL2/ADSL2/2+ capabilities on an HWIC form factor for the ISR G2 series.

For more information, see the following documents:

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/dsl_hwic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/inst_ic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/oview_ic.html

<http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html>

Enhanced Cisco 880 Wireless Platforms (C881W-A-K9, C881W-E-K9, C881W-P-K9, C886VA-W-E-K9, C887MVA-W-E-K9, C887VA-W-A-K9, C887VA-W-E-K9)

For more information, see the following document:

http://www.cisco.com/en/US/partner/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html

New Software Features Supported in Cisco IOS Release 15.1(4)M

This section describes new and changed features in Cisco IOS Release 15.1(3)T3. Some features may be new to Cisco IOS Release 15.1(3)T3 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T3. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed is available in the feature description provided.

Call Escalation from Voice to Video

For more information, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html>

Cisco IOS NAM PA for WAAS Express

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_ios_nam_pa_waas.html

Cisco IOS Shell

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_ios_shell.html

Cisco ISR G2 Multi Gigabit Fabric Phase 2

For more information, see the following document:

<http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/mgfcfg.html>

Cisco Unified CME 8.6

For more information, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Cisco V.150.1 Minimum Essential Requirements

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html

CUBE Lite on Cisco 800 Series ISR

CUBE features like SIP-to-SIP Delayed-Offer/Early-Offer calls, SRTP calls in pass-through mode, and basic SIP to H.323 calls are supported on CUBE Lite platform (Cisco 880 and Cisco 890 platforms).

DHCP User Auth CLI for FORCERENEW

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_client.html

DMVPN Event Tracing

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_dmvpn_event_trace.html

EIGRP IPv6 VRF-Lite

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_cfg_eigrp.html

Flexible NetFlow—32-Bit AS Number Support

With Cisco IOS Release 15.1(4)M, Flexible NetFlow supports 32-bit autonomous system (AS) numbers. Flexible NetFlow can capture and export 32-bit numbers as well as 16-bit numbers. If you specify the 4-octet keyword in the collect routing or match routing command, you configure the 32-bit autonomous system number as a nonkey or key field; otherwise, you configure the 16-bit version. If you configure both a 32-bit version and a 16-bit version within a record, only the 32-bit version applies. The 32-bit AS numbers have a different v9 export type than that used for 16-bit AS numbers. Your collector and analysis infrastructure should be able to process values for 32-bit AS numbers.

The following commands have been added in this release to support this feature:

[match | collect] **routing destination as** [4-octet]

[match | collect] **routing destination as peer** [4-octet]

[match | collect] **routing source as** [4-octet]

[match | collect] **routing source as peer** [4-octet]

For more information on export types, see the *NetFlow Layer 2 and Security Monitoring Exports* document:

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/nf_lay2_sec_mon_exp.html

IPv4 MIB Support (RFC 4293)

Cisco IOS Release 15.1(4)M includes support for the IPv4 MIB as described in RFC 4293, Management Information Base for the Internet Protocol (IP). As part of this support, the **clear ip traffic** command and the **show ip traffic** command were modified. For more information about these commands and their modifications, see the *IP Application Services Command Reference* and the *IP Switching Command Reference*.

http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html

http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_book.html

IPv6 Multicast VRF Lite

For more information, see the following document:

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html>

IPv6 Support for IPSec and IKEv2

Cisco IOS Release 15.1(4)M provides IPv6 support for IKEv2 and IPSec protocols. This is in accordance with the US Government's IPv6 certification requirements. This release implements IPv6 support for crypto maps and tunnel protection.

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_vpn_ipsec.html

LISP Locator/ID Separation Protocol

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/15-1mt/irl-15-1mt-book.html

MAC Authentication Bypass (MAB)

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_config_mab.html

MVPN—Data MDT Enhancements

Multicast distribution tree (MDT) groups were selected at random when the traffic passed the threshold and there was a limit of 255 MDTs before they were reused. The MVPN—Data MDT Enhancements feature provides the ability to deterministically map the groups from inside the VPN routing and forwarding (S,G) entry to particular data MDT groups, through an access control list (ACL). The user can now map a set of VPN routing and forwarding (S,G) to a data MDT group in one of the following ways:

- 1:1 mapping (1 permit in ACL)
- Many-to-1 mapping (many permits in ACL)
- Many-to-many mapping (multiple permits in ACL and a nonzero mask data MDT)

Because the total number of configurable data MDTs is 1024, the user can use this maximum number of mappings in any of the described combinations.

OSPF—Demand Circuit Disable

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_cfg.html

PPPoE—Max-Payload Support on Client

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/bbds1/configuration/guide/bba_ppoe_client.html

Product Security Baseline—Password Encryption and Complexity Restrictions

This feature introduces the `aaa password restriction` command, which enforces that passwords be subject to the following restrictions:

- The new password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters
- The new password should not have a character repeated more than three times consecutively
- The new password should not be the same as the associated username. A password obtained by capitalization of the username or username reversed is not accepted
- The new password should not be "cisco," "ocsic," or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "l" or "!" for i, or by substituting "0" for "o", or substituting "\$" for "s."

The restrictions can be applied to the passwords configured using the following commands: **aaa pod server**, **enable password**, **enable secret**, **radius-server key**, **radius-server host key**, **server-key**, and **tacacs-server key**.

Radius Statistics VIA SNMP

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_radius.html

Secure Tone Support on MGCP TDM GW

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/mgcp/configuration/guide/vm_secure_tone.html

SIP Loopback Support

For more information, see the following document:

<http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html>

USB Enable/Disable for Cisco ISR Routers

Feature Introduction

The USB Disable feature provides Cisco IOS administrators with the ability to disable all USB ports on the router.

Default Setting

Cisco IOS enables USB ports by default, which preserves existing USB functionality such as the following:

- Booting the Cisco IOS from a USB port
- Saving configuration files to a router for Cisco IOS reloads



Note Using the USB Disable feature (to disable or re-enable the USB ports) requires a router reboot. When USB ports are disabled from within Cisco IOS, USB functionality remains unavailable until re-enabled.

For more information, see the following document:

http://www.cisco.com/en/US/docs/solutions/GGSG-Engineering/15_1_4M/USB_Disable.html

Video Conferencing Services on Cisco Integrated Services Router G2

This release enhances the existing audio conferencing and transcoding feature set by adding support for video conferencing on Cisco Integrated Services Router Generation 2 (ISR G2). This ISR G2 uses on-board Digital Signal Processor (DSP) resources (Packet Voice Video Digital Signal Processor Module PVDM3) combined with Cisco IOS software to switch a scalable number of ad hoc or MeetMe video conference calls for Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

For more information, see the following document:

http://www.cisco.com/en/US/products/sw/voicesw/ps4952/products_installation_and_configuration_guides_list.html

ZBFW Support for MSRPC

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_zone_policy_firew.html

Important Notes

The following information applies to all releases of Cisco IOS Release 15.1(4)M:

- [Cisco IOS Behavior Changes](#), page 90
- [Important Notes for Cisco IOS Release 15.1\(4\)M3](#), page 99
- [Important Notes for Cisco IOS Release 15.1\(4\)M1](#), page 100
- [Important Notes for Cisco IOS Release 15.1\(4\)M](#), page 101

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- [Cisco IOS Release 15.1\(4\)M6, page 90](#)
- [Cisco IOS Release 15.1\(4\)M5, page 91](#)
- [Cisco IOS Release 15.1\(4\)M4, page 92](#)
- [Cisco IOS Release 15.1\(4\)M3, page 94](#)
- [Cisco IOS Release 15.1\(4\)M2, page 95](#)
- [Cisco IOS Release 15.1\(4\)M1, page 97](#)

Cisco IOS Release 15.1(4)M6

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M5:

- BGP processing of the removal of private AS numbers from the AS path.

Old Behavior: When the **neighbor remove-private-as** command is configured and a route-map without a continue clause is configured, the processing order is:

- neighbor remove-private-as processing
- set as-path prepend or set as-path prepend last-as

However, if the route-map contains a continue clause, the processing order is reversed.

New Behavior: When the **neighbor remove-private-as** command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:

- neighbor remove-private-as processing
- set as-path prepend or set as-path prepend last-as

- RTP signal processing is disabled by default.

Old Behavior: RTP packets of payload type ?123? can cause errors on Cisco AS5350 and AS5400 series platforms.

New Behavior: RTP signal processing is disabled by default to prevent errors caused by RTP packets of payload type “123” and can be enabled when necessary using the **voice-fastpath voice-rtp-signalling enable** command.

Additional Information:

http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800a96c1.shtml

- Improper tunnel MTU value.

Old Behavior: The IPsec encapsulation bytes are calculated based on the source interface.

New Behavior: The IPsec encapsulation bytes are calculated based on the outgoing physical interface.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/ip_inspect_through_ip_security_strip.html#GUID-6BED3794-8050-4464-9A17-8D8C8C02EF88

- Setting of factory defaults.

Old Behavior: When the push button is pressed, configuration and image recovery takes place at WLAN AP running on 2nd core of next generation c8xx platforms.

New Behavior: When the push button is pressed, ONLY configuration recovery takes place at WLAN AP running on 2nd core of next generation c8xx platforms.

- A new keyword is added to the **timers** command.

Old Behavior: The **dns** keyword is not available with the **timers** command.

New Behavior: The **timers** command can use the **dns** keyword.

Additional Information: <http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr5/vcr-t2.html>

Cisco IOS Release 15.1(4)M5

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M5:

- Change to how IPv6 paths are advertised.

Old Behavior: An IPv6 path is advertised without a label when the label has not been negotiated

New Behavior: IPv6 paths are not advertised if the label has not been negotiated

- The SIP call hold/resume scenario has been enhanced so that the RTP sequence number is continuous from the origin of the call until the end.

Old Behavior: The RTP sequence number is not continuous from the origin until the end of a SIP call, including the time when the call is on hold.

New Behavior: The RTP sequence number is now continuous from the origin until the end of a SIP call.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-1mt/voi-sipsip-sbc.html

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-2mt/voi-sipsip-sbc.html

- The prompt command is made available on the Cisco 860 series, 860VAE series, and 880 series routers.

Old Behavior: The Cisco 860 series, 860VAE series, and 880 series routers do not support the prompt command.

New Behavior: The prompt command is available on these routers.

- PfR syslog levels have been added to minimize the number of messages.

Old Behavior: Too many PfR syslog messages are generated.

New Behavior: PfR syslog levels have been added to minimize the number of messages displayed and a syslog notice has been added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html>

- In the IPsec SVTI configuration with HA, existing security associations are not affected.

Old Behavior: When configuring IPsec SVTI with HA, the standby router reload interrupts the existing security associations.

New Behavior: When configuring IPsec SVTI with HA, the standby router reload does not affect the existing security associations.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-2mt/sec-ipsec-virt-tunnl.html#GUID-D4B2DE6B-A9B1-4F68-AF39-995CDAFFDEB9

- An early warning is displayed on the CPU for over temperature case.

Old Behavior: There is no early warning displayed on the CPU for over temperature case.

New Behavior: There is an early warning displayed on the CPU for over temperature case.

- The **clear call threshold interface** command can be used for a Gigabit Ethernet interface.

Old Behavior: Unable to the **clear call threshold interface** command for a Gigabit Ethernet interface.

New Behavior: Gigabit Ethernet interface is a valid interface type.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr-c5.html#GUID-63581F18-D001-4975-A04E-9A0807CAB08E>

- HQF shape timer can replenish the shape tokens at 1 ms or 4 ms intervals.

Old Behavior: The Hierarchical Queuing Framework (HQF) shaper timer replenishes the shape tokens at 4-millisecond (ms) intervals.

New Behavior: The **qos shape-timer** command allows you to configure the HQF shaper timer to replenish the shape tokens at 1-ms or 4-ms intervals.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/Q_through_R.html

Cisco IOS Release 15.1(4)M4

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M4:

- Connected number and Connected name are sent in an ISDN CONNECT message as Connected Number IE and Connected Name (display IE).

Old Behavior: Connected number and Connected name that are signaled to the Cisco IOS software from a SIP 200 OK message are not sent in an ISDN CONNECT message.

New Behavior: Connected number and Connected name that are signaled to the Cisco IOS software from a SIP 200 OK message are sent as Connected Number IE and Display IE (Connected Name) in the ISDN CONNECT message. Passing the Connected number and the Connected name is enabled by configuring the following commands in interface configuration mode: **isdn outgoing ie connected-number**, **isdn outgoing ie display**.

Additional Information:

http://www.cisco.com/en/US/docs/ios/dial/command/reference/dia_i2.html

- Change in BGP next-hop for redistributed recursive static routes.

Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be itself. The local next-hop (equal to next-hop-self) is kept.

New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.

- A new keyword is added to the **supplementary-service sip** command.
 Old Behavior: The *handle-replaces* keyword is not available in the **supplementary-service sip** command.
 New Behavior: The *handle-replaces* keyword is available for the **supplementary-service sip** command.
 Additional Information:
<http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr4/vcr-s12.html#GUID-98E8D5E4-A18F-49D4-ACC7-8104E01A0C1A>
- New keywords **standard** and **system** are added to the existing **dtmf-interworking** CLI under voice service and dial-peer configuration modes.
 Old Behavior: SIP INFO dtmf digit to RFC4733 DTMF interworking was not supported.
 New Behavior: The newly added keyword **standard** generates RTP NTE packets that are RFC 4733 compliant.
 Additional Information:
<http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-d2.html#GUID-ED049ED0-50B0-4C38-B3EE-7DDE625389F4>
- Added analogue vm-integration in SIP line
 Old Behavior: vm-integration only applies to SCCP line.
 New Behavior: vm-integration also applies to SIP line.
 Additional Information:
http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/srst_voicemail.html
- PfR syslog levels are added to minimize number of messages.
 Old Behavior: There are too many PfR syslog messages.
 New Behavior: PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.
 Additional Information:
<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html>
- Connected number and Connected name are sent in an ISDN CONNECT message as Connected Number IE and Connected Name (display IE).
 Old Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are not sent in an ISDN CONNECT message.
 New Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are sent as Connected Number IE and Display IE (Connected Name) in the ISDN CONNECT message. Passing the Connected number and the Connected name is enabled by configuring the following commands in interface configuration mode: **isdn outgoing ie connected-number**, **isdn outgoing ie display**.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/dial/command/reference/dia_i2.html
- Answer (ANS) tone treatment is enabled for modem and fax answer tone.
 Old Behavior: There is no ANS tone treatment enabled for modem and fax answer tone.
 New Behavior: The ANS tone treatment can be enabled for modem and fax answer tone by using the *ans-treatment* keyword in the **fax-relay** command.

Additional Information: <http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-f1.html>

- Fast Network Time Protocol (NTP) synchronization is achieved.

Old Behavior: The burst and initial burst (iburst) modes are enabled manually.

New Behavior: The burst and iburst modes are enabled by default.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-CC69EFC5-68A3-4C5D-90CD-67DE45D4A370>

Cisco IOS Release 15.1(4)M3

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M3:

- CLI introduced to ignore S1 SONET overhead byte set to 0xF

Old Behavior: A packet received with an S1 SONET overhead byte set to 0xF causes the router to switch the clock source to internal.

New Behavior: A CLI **atm sonet ignore s1** has been introduced, which when set directs the router to ignore an S1 overhead byte set to 0xF, which in turn ensures that the clock does not change.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/atm/command/atm-a1.html>

This CLI is currently applicable only on ASR1K. This CLI will be visible but not enabled on other platforms.

- The **do** configuration command has been reactivated for Cisco IOS Release 15.x.

Old Behavior: The **do** command had been removed temporarily.

New Behavior: The **do** command is now reactivated.

Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-7E54B6C8-BA6F-4B0E-8A7B-19B50E66042A

- BGP scan time range is changed

Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15-60 seconds. The **bgp scan-time** command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

New Behavior: The **bgp scan-time** command has a scanner-interval range of 5-60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

- Increase in autonomous system number or community prepending in BGP Inbound Optimization using PfR.

Old Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the number is increased one by one up to the maximum of six ASes in unreachable, loss, and delay OOP cases.

New Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the new behavior increases the AS number or community to the maximum of six immediately, for unreachable and loss OOP cases.

In the delay OOP case, the behavior is the same as the old behavior.

Additional Information: See the “PfR Entrance Link Selection” section under Information About in:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-2mt/pfr-bgp-inbound.html>

- Increased maximum number of traffic classes (prefixes) to be learned in a PfR learn list.

Old Behavior: Using the Cisco IOS CLI, **count** (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list was 100, with a default of 50.

New Behavior: Using the Cisco IOS CLI, **count** (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list is 1000, with a default of 1000.

Additional Information: The command is documented in the Performance Routing Command Reference at:

<http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html>

- ADSL interface fails to retrain when the **dsl enable-training-log** command is configured.

Old Behavior: When the **dsl enable-training log** command is configured and a cable is disconnected from an asymmetric digital subscriber line (ADSL) card and then reconnected, the ADSL interface fails to retrain.

New Behavior: To prevent this from happening, disable the retrieval of the DSL training log using the **no dsl enable-training-log** command. The DSL will now train up to the DSLAM.

Additional information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/bbds1/command/bba-a1.html>

- Netmask should be specified while configuring the svc address pool under policy group.

Old Behavior: Netmask was optional while configuring the svc address pool under policy group.

New Behavior: Netmask keyword is made mandatory while configuring the svc address pool.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s6.html#GUID-4AB61E8E-4D2E-4A5B-9943-6AD1F90FF572>

Cisco IOS Release 15.1(4)M2

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M2:

- The **logging source-interface** command needs new VRF information for customer ease of use.

Old Behavior: Users could not configure VRF information when using the **logging source-interface** command.

New Behavior: The **vrf** keyword and *vrf-name* argument are supported in the Cisco IOS Releases 12.2(33)SXJ1 and 15.1(3)S.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_09.html

- Change to **neighbor prefix-length-size** command

Old Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, if that neighbor has a peer policy or route map that is removed, the **neighbor prefix-length-size** command setting is also removed.

New Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, the value of that command overrides the value set for the peer-group. If the command is locally configured for the peer, it will not be inherited from the peer-group.

- Change in **show bgp ipv4 unicast summary** command

Old Behavior: The **show bgp ipv4 unicast summary** command displays an incorrect number of dynamically created neighbors per address family if a peer-group has been removed from the configuration.

New Behavior: The **show bgp ipv4 unicast summary** command displays the correct number of dynamically created neighbors, even if a peer-group has been removed. The output displays the number of dynamically created neighbors per address family, and at the end of output, displays the total number of dynamically created neighbors on the router.

- **Batch** command available under interface mode.

Old Behavior: **batch** command was not available under interface.

New Behavior: **batch** command is available under interface

Additional Information:

<http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/routconf.html>

- The **cable-detect** command does not support analog FXO ground-start voice port. The command must be documented with this information.

Old Behavior: The **cable-detect** command can be configured on analog FXO loop-start, ground-start and cama voice port.

New Behavior: The **cable-detect** command cannot be configured on analog FXO ground-start voice port. This command is supported only for analog FXO loop-start and cama voice port.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr1-cr-book.html>

- Tunnel transport MTU now accounts for IPsec encryption with GRE

Old Behavior: The tunnel transport maximum transmission unit (MTU) did not account for IPsec encryption overhead with generic routing encapsulation (GRE). The tunnel transport MTU is used to fragment the packet. Since the transport MTU reduces, some packets that were previously fragmented post encryption are fragmented at the tunnel interface.

New Behavior: The tunnel transport MTU now accounts for IPsec encryption overhead with GRE. Use the **show interfaces tunnel** command to see updated command output for a tunnel interface.

- Power down time for the SRE module.

Old Behavior: SRE module takes two minutes to power down.

New Behavior: If the SRE module is not running an application, the time-out interval is less than two minutes. If the SRE module is running an application, it requires a 2-minute time-out interval to reflect the actual change in Cisco EnergyWise level.

Additional Information:

http://www.cisco.com/en/US/docs/routers/access/1900/software/configuration/guide/enrgyz_artg.html

- Documentation changes to support Optimized Edge Routing (OER) CLI hidden in Cisco IOS Release 15.0(1)SY

Old Behavior: OER border router functionality was supported on the Catalyst 6500 Switch.

New Behavior: OER is no longer supported on the Catalyst 6500 Switch, and the OER CLI is hidden in Cisco IOS Release 15.0(1)SY.

Additional Information:

<http://www.cisco.com/en/US/docs/ios-xml/ios/oer/command/oer-cr-book.html>

- Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.
Old Behavior: Analog (FXS) phones connected to Cisco IAD2430 are not recognized as SCCP endpoints.
New Behavior: Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.
Additional Information:
<http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fxssccpsplmft.html>

Cisco IOS Release 15.1(4)M1

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M1:

- PPPoA SSO for forwarded sessions is not supported.
Old Behavior: PPPoA SSO for forwarded sessions on LAC is not supported.
New Behavior: PPPoA SSO for forwarded session is supported. The output of the show pppatm redundancy command is modified to display the number of PPPoA sessions that are forwarded and synced to the standby Route Processor (on the active RP) and forwarded and re-created on the standby RP.
- Input service policies are not implemented for PPPoE client traffic.
Old Behavior: Input service policies attached to a main interface or a subinterface are not implemented for PPPoE client traffic. Only input service policies attached to a dialer interface are implemented.
New Behavior: Input service policies attached to a main interface or a subinterface are implemented for PPPoE client traffic but only if an input service policy is not configured for a dialer interface. If an input service policy is configured for a dialer interface, the old behavior is retained. Only the quality of service (QoS) counters for packet classification are supported. Counters for packet dropping, packet marking, and policing actions are not supported and are ignored.
- BGP no longer activates IPv6 peers in IPv4 address family automatically.
Old Behavior: By default, both IPv6 and IPv4 capability is exchanged with a BGP peer that has an IPv6 address. When an IPv6 peer is configured, that neighbor is automatically activated under the IPv4 unicast address family.
New Behavior: Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under the IPv4 address family, you can manually deactivate the peer with the no neighbor ipv6-address activate command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.
Additional Information:
http://www.cisco.com/en/US/partner/docs/ios-xml/ios/iproute_bgp/configuration/15-1mt/irg-basic-net.html
http://www.cisco.com/en/US/partner/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_basic_net_xe_ps11174_TSD_Products_Configuration_Guide_Chapter.html
- The **ip header-compression old-iphc-comp** and **ip header-compression old-iphc-decomp** commands are added to configure the IPHC format of compression and decompression to the non-RFC-compliant format.
Old Behavior: The header compression decodes RTP timestamp incorrectly. This issue occurs mainly with IPHC format compression interacting with older IOS releases.

New Behavior: The **ip header-compression old-iphc-comp** and **ip header-compression old-iphc-decomp** commands are used to revert the IPHC format of compression and decompression to the non-RFC-compliant format.

Additional Information:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_i1.html#wp1065764

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_i1.html#wp1066790

- Routing protocols purge routes when an interface goes down.

Old Behavior: Routing protocols do not purge routes when an interface goes down. This is the default behavior.

New Behavior: Routing protocols purge routes when an interface goes down. This is the default behavior.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1013065

- The hold-alert notification period is not adjustable after first timeout.

Old Behavior: The hold-alert notification period is not adjustable after first timeout.

New Behavior: The hold-alert notification period is adjustable after first timeout. The recurrence <recurrence-timeout> parameter has been added.

Additional Information:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_h1ht.html#wp1021169

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmering.html#wp1013688

- The **ntp panic update** command is introduced.

Old Behavior: There is no command to configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds.

New Behavior: A new command, **ntp panic update**, has been introduced to configure NTP to reject time updates greater than the panic threshold of 1000 seconds. If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

```
NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000.
seconds; set clock manually to the correct UTC time.
```

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html

- A change has been made to the CLI command output.

Old Behavior: The command output does not display the bundled WLAN AP bootloader version.

New Behavior: The command output displays the bundled WLAN AP bootloader version.

- A new command, **cdma ddtm**, is added.

Old Behavior: On CDMA modems, data transmission is disrupted by incoming voice calls if data dedicated transmission mode (DDTM) is disabled.

New Behavior: The **cdma ddtm** command enables DDTM.

Additional Information:

<http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwlcdma.html>

- If there is cause for an IKE registration security association to be deleted on a GDOI group member, it will also be deleted for all groups that share it.

Old Behavior: When an IKE registration SA is shared among multiple GDOI groups, it is not consistently cleared on members of all groups.

New Behavior: If there is cause for an IKE registration SA to be deleted on a group member (even if another group is still running and has previously registered through it), it will be deleted for all groups.

Additional Information:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

- The flow direction field can now be exported by Cisco Performance Monitor.

Old Behavior: The flow direction field was not exported by Cisco Performance Monitor.

New Behavior: The **collect flow direction** command can now be used to export the flow direction field along with the other performance data being monitored.

Additional information:

http://www.cisco.com/en/US/docs/ios/media_monitoring/command/reference/mm_perf_mon.html

and

http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/15_1m_and_t/mm_15_1m_and_t.html

- There is a change in the CLI output.

Old Behavior: When the netflow cache size is other than the default (64K), netflow needs to be reenabled at all applicable interfaces to take effect.

New Behavior: After every reboot the configured netflow cache size is applied from the startup configuration. There is a change of configuration order for “ip flow-cache entries xxxxx” and “ip flow-egress input-interface”; the **show running configuration** command now reflects this change.

Important Notes for Cisco IOS Release 15.1(4)M3

This section describes important issues that you should be aware of for Cisco IOS Release 15.1(4)M3 and later releases.

Cisco Images Deferred

In Cisco IOS Release 15.1(4)M3, 24 images have been deferred. This defect has been assigned Cisco caveat ID CSCtx06747. The affected images are as follows:

c5350-ik9s-mz

c5350-ik9su2-mz

c5350-jk9s-mz

c5350-jk9su2_ivs-mz

c5400-ik9s-mz

c5400-ik9su2-mz

c5400-jk9s-mz

c5400-jk9su2_ivs-mz

c7200-adventerprisek9-mz
c7200-adventerprisek9_sna-mz
c7200-advipservicesk9-mz
c7200-advipservicesk9_li-mz
c7200-advsecurityk9-mz
c7200-ipbasek9-mz
c7200-spservicesk9-mz
c7200p-adventerprisek9-mz
c7200p-adventerprisek9_sna-mz
c7200p-advipservicesk9-mz
c7200p-advipservicesk9_li-mz
c7200p-advsecurityk9-mz
c7200p-ipbasek9-mz
c7200p-spservicesk9-mz
vgd-jk9s-mz
vgd-jk9su2_ivs-mz

The software solution for these deferred images is Cisco IOS Release 15.1(4)M3a. The DDTS Solution is CSCtx06747 (Headline: Boot failure due to TLB (Store) Exception with ASSERTION FAILED logged).

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.



Note

Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images, will apply to the replacement images.

Important Notes for Cisco IOS Release 15.1(4)M1

This section describes important issues that you should be aware of for Cisco IOS Release 15.1(4)M1 and later releases.

Cisco Security Manager

The Cisco Connected Grid 2010 router supports Cisco Security Manager. For more information, see the *Cisco Security Manager Configuration Guides*:

http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html

Gateway Crash When SIP-KPML Signaling Is Configured in SIP Gateway Dial Peers (CSCtq56727)

There is a defect in Cisco IOS Release 15.1(4)M when the configuration in Unified Communications Manager that is pointing to a SIP gateway is set with DTMF signaling type as “no preference” and the SIP gateway is configured with DTMF relay as sip-kpml.

Bulk call failures are seen during heavy loads of traffic and are followed by a gateway crash. The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP and other processes.

The show processes memory sorted command shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

There are two workarounds:

1. Set the DTMF signaling type as “OOB and RFC 2833” in Unified Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
2. Configure “dtmf-relay rtp-nte” at the SIP gateway dial-peer configuration, instead of “sip-kpml.” The Unified Communications Manager is configured with “no preference.”

In order to recover from the crash, the gateway router must be reloaded.

Important Notes for Cisco IOS Release 15.1(4)M

This section describes important issues that you should be aware of for Cisco IOS Release 15.1(4)M and later releases.

Video Conferencing Services on the Cisco Integrated Services Router G2

The following section describes some important information about the video conferencing and transcoding feature.

- For a Cisco Unified IP Phone 7985 that is registered with Cisco Unified CME to participate in a video conference, the phone requires a DSP farm profile that is configured with the H.263 codec. Cisco Unified IP Phones 7985 connected to Cisco Unified Communications Manager can support both H.263 and H.264.
- Cisco Unified IP Phones 9951 and 9971 have the following interoperability issues:
 - Cisco Unified IP Phones 9951 and 9971 require a DSP farm profile that is configured with the H.264 codec.
 - When you enable the lecture mode option on Cisco Unified CME, a conferee on Cisco Unified IP Phones 9951 and 9971 cannot become a lecturer. Users on the phone can only participate in the video conference as conferees.
 - Cisco Unified IP Phones 9951 and 9971 use the Real-Time Transport Protocol (RTP) payload value of 97. This value is often reserved for cisco-codec-fax-ack. You must reconfigure your RTP payload for cisco-codec-fax-ack and for cisco-codec-video-h264 by adding the following commands to the appropriate dial-peer profile:


```
rtp payload-type cisco-codec-fax-ack 111
rtp payload-type cisco-codec-video-h264 97
```
- Lifesize endpoints using 4cif resolution display a blank screen when a conferee on a Cisco Unified IP Phone 9951 or 9971 with qcif resolution becomes the active speaker. The display correctly displays all other conferees.

- Ad hoc conferences on endpoints that are connected through a SIP trunk are currently not supported. However, endpoints that are connected through a SIP trunk can connect to MeetMe video conferences.



Caveats for Cisco IOS Release 15.1(1)T

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- [Resolved Caveats—Cisco IOS Release 15.1\(1\)T5, page 104](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(1\)T4, page 111](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(1\)T3, page 136](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(1\)T2, page 153](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(1\)T1, page 167](#)
- [Open Caveats—Cisco IOS Release 15.1\(1\)T, page 188](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(1\)T, page 216](#)



Resolved Caveats—Cisco IOS Release 15.1(1)T5

Cisco IOS Release 15.1(1)T5 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T5 but may be open in previous Cisco IOS releases.

- CSCsx87562

Symptoms: The following error is seen following interface range configuration change:
 %SYS-3-TIMERNEG: Cannot start timer (0XXXXXXXX) with negative offset (- YYYYYYYYYY).
 -Process= "<interrupt level>", ipl= 2

Conditions: This symptom is seen with dual supervisors installed and affects the following Cisco Catalyst 4000 releases: Cisco IOS Release 12.2(52)SG/XO, Cisco IOS Release 12.2(50)SG4/5/6/7, and Cisco IOS Release 12.2(53)SG/SG1/SG2. This bug applies to all hardware, and is not specific to Cisco Catalyst 4500 series switches.

Workaround 1: Configure the interfaces one by one.

Workaround 2: Force a switchover "redundancy force-switchover".

Workaround 3: Use Cisco IOS Release 12.2(50)SG3 until the fix code is released.

Resolution: The fix is available in Cisco IOS Release 12.2(54)SG which is available to download on CCO. The fix will also be in Cisco IOS Release 12.2(53)SG3 and Cisco IOS Release 12.2(50)SG8.

- CSCte53162

Symptoms: In radius messaging, nas-port-id is not prepended to "acct-session-id" when the **nas-port format e encoding string** command is configured.

Conditions: This symptom is observed when the **nas-port format e encoding string** command is configured.

Workaround: Use the **nas-port format d encoding bits** command.

- CSCte97113

Symptoms: The **configure replace** command fails and crashes the standby when you try to replace an existing configuration on the active that has parser views configured with a configuration that does not have any parser views configured.

Conditions: This symptom is observed when the user is in root view mode while configuring a parser view. During configure replace, the standby is not set into root view mode.

Workaround: Manually remove/configure the parser view on the active to match with what it is in the saved configuration before opting for configure replace.

- CSCtf49537

Symptoms: During the bulk-sync, Standby does not reload when a configuration command with parser return code error is seen on Standby. The user will not notice if a PRC error occurred.

Conditions: This symptom is observed when the PRC error result status is not sent back from Standby to Active properly.

Workaround: After the system reaches the SSO state, issue the following exec command via the Active console to check if PRC error occurred.

```
router# show redundancy config-sync failures prc
```

- CSCtf71990

Symptoms: An alert message is not sent if "source-ip-address" is configured in the call-home configuration. The following message is shown:

```
%CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP
```


servers (ERR 7, error in connecting to SMTP server)

Conditions: The symptom is observed when “source-ip-address” is configured.

Workaround: Remove “source-ip-address”.

- CSCtg79262

Symptoms: A Cisco IOS Embedded Event Manager (EEM) Tool Command Language (Tcl) policy can get stuck in the EEM active scheduler queue. The policy will consume a scheduler thread and cannot be cleared automatically by the maxrun timer or manually using the EEM exec command **event manager scheduler clear all**.

Conditions: This symptom occurs in very rare circumstances. For example, if the system has enough memory to schedule and start running the EEM policy, but the policy fails due to a lack of memory.

Workaround: The only way to recover is to reload.

- CSCtg91572

Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

Workaround: There is no workaround.

- CSCth43911

Symptoms: The system may crash when performing the SNMP SET operation for CISCO-CALLHOME-MIB objects in callHomeDestEmailAddressTable, ccmSeverityAlertGroupTable, ccmPeriodicAlertGroupTable, ccmPatternAlertGroupTable, ccmEventAlertGroupTable, and ccmDestProfileTestTable.

Conditions: This symptom does not occur under any specific conditions.

Workaround: There is no workaround. The fix exists in Cisco IOS Release 12.2(33)SXJ and Cisco IOS Release 12.2(50)SY.

- CSCth61759

Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate the video stream.

Conditions: This symptom is observed in two scenarios:

Scenario 1: This symptom was observed in the following SIP-SIP Delayed Offer-Delayed Offer (DO-DO) call flow :

```
7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server
```

1. Call is originated by 7985.
2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response.

```
m=video 53722 RTP/AVP 96 97 34 31
b=AS:1920
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600
a=rtpmap:97 H263-1998/90000
a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1
a=rtpmap:31 H261/90000
a=fmtp:31 CIF=1;QCIF=1
```

```
a=sendrecv
```

3. CUBE sets video m-line to 0 in the SDP of the SIP “ACK” response

```
m=video 0 RTP/AVP 96
```

Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

```
CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA
```

Workaround: There is no workaround.

- CSCth84370

Symptoms: The Standby Supervisor gets reloaded when **write memory** is run from one VTY, and then later, **show configuration** is run from another VTY. No particular configuration needs to be done prior to **write memory**.

Conditions: This symptom occurs when the Dual Supervisor is used and the configuration file is quite long.

Workaround: Do not run the **write memory** and **show configuration** commands simultaneously.

- CSCth92828

Symptoms: When viewing a device configuration, such as via a URL like https://tools.cisco.com/sch/reports/viewDeviceConfiguration.do?specific_item_query, the TACACS server key, a type 7 reversible password, is still visible.

Conditions: This symptom is observed when viewing a device configuration.

Workaround: There is no workaround.

- CSCti08811

Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

Conditions: This symptom is observed only with EEM policies.

Workaround: There is no workaround.

- CSCti41891

Symptoms: When 812 tunnels are configured, Standby starts rebooting.

Conditions: This symptom is observed with scalability.

Workaround: There is no workaround.

- CSCti46171

Summary: The Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets.
- Memory Leak in HTTP Inspection.
- Memory Leak in H.323 Inspection.
- Memory Leak in SIP Inspection.

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The

Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2012-1315 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtj48387

Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP-related errors.

Conditions: This symptom occurs when DHCP is enabled and sessions get DHCP information from a RADIUS server.

Workaround: There is no workaround.

- CSCtn55070

Symptoms: Call-home http messages can hang and not be sent out.

Conditions: This symptom is observed when call home is enabled and an http transport method is used. This symptom is timing-dependent and cannot be hit every time. In addition, this symptom is observed in telnet sessions.

Workaround: Log in to the console port if a telnet session was used to send call-home http messages. Because the console is waiting on user-supplied information (--More--), enter something into the console; the call-home process can then continue to execute.

- CSCtq06538

Symptoms: A Cisco ASR with a route processor 2, running Cisco IOS XE, may experience RP crashes due to bad chunk in MallocLite.

Conditions: This symptom occurs while executing Codenomicon BGP tests.

Workaround: There is no workaround.

Additional Information: This crash was only seen in some 15.x versions of Cisco IOS XE. It is due to a malformed BGP attribute received from a valid BGP neighbor. This attribute is not passed on to any systems other than the vulnerable router.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.7/4.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C>

CVE ID CVE-2012-1367 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq45553

Summary: The Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets.
- Memory Leak in HTTP Inspection.
- Memory Leak in H.323 Inspection.
- Memory Leak in SIP Inspection.

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2012-0388 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq92650

Symptoms: DMVPN tunnel is not selecting the right source interface.

Conditions: The symptom is observed when multi-link frame relay creates more than one sub-interface with the same name.

Workaround: There is no workaround.

Further Problem Description: This bug resolves the issue reported in CSCth08338 for Cisco IOS Release 15.1M.

- CSCtr28857

Summary: A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of the Cisco IOS Software and the Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr54327

Symptoms: A Cisco router may crash due to a SegV exception or may have spurious access when a fax comes in.

Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the "a=silenceSupp:off" option is set in SDP.

Workaround: Disable fax by going into the “voice service voip” mode and configuring the **fax protocol none** command.

- CSCts38429

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike>

Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

- CSCts80643

The Cisco IOS Software and the Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

A workaround is available to mitigate this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp>

- CSCtt11210

Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, and not the subject-name as it would be expected.

Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt94391

Symptoms: A Cisco wireless router may unexpectedly reboot due to a bus error with the following error leading up to the crash:

```
ASSERTION FAILED: file '../dot11t/t_if_dot11_hal_ath.c', line XXXX
```

Conditions: This issue relates to the wireless on the router. This crash can be seen on the following platforms: Cisco 870W, 1800W, UC500W, and 2800 and 3800 routers with HWIC-AP. The crash is only seen when an iPhone 4S is connected to the router. The crash has most commonly been triggered by running a video call application on the phone, but there may be other triggers. Other than the wireless configuration and other generic configurations needed to provide connectivity to the router, no other specific configuration is needed to see the crash.

Workaround: There is no workaround on the router. However, this issue is not seen with an iPhone 4s running iOS 5.1. The issue is only seen on iOS 5.0.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C>

CVE ID CVE-2012-1327 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtu02835

Symptoms: While running Cisco IOS Release 15.1(4)M2, slow performance is exhibited through the Fast Ethernet WAN ports.

Conditions: This symptom is observed when the **scheduler interval** command is configured. This causes the Fast Ethernet WAN ports to display many throttles in the **show interface** command.

Workaround: Remove the **scheduler interval** command.

- CSCtu36224

Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.

Workaround: There is no workaround.

- CSCtx38806

Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

The problem affects Firefox also (version 10.0.1) displaying the following message:

"The page isn't redirecting properly."

Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.

Workaround: Any of the following workarounds will work:

1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
2. Uninstall the update.
3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

```
webvpn gateway gateway name
    ssl encryption rc4-md5
```

4. Use AC 2.5.3046 or 3.0.3054.
5. Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:

"Connection attempt has failed due to server communication errors. Please retry the connection."

The AnyConnect event log will show the following error message snippet:

Function: ConnectIfc::connect
 Invoked Function: ConnectIfc::handleRedirects
 Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCty42626

Symptoms: Certificate enrollment fails for the Cisco 3945 router and the Cisco 3945E router due to digital signature failure.

Conditions: This symptom is observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

Workaround: There is no workaround.

- CSCty43587

Symptoms: A crash is observed with memory corruption similar to the following:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc
XXXXXXXX, dealloc XXXXXXXX
```

Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(1)T4

Cisco IOS Release 15.1(1)T4 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T4 but may be open in previous Cisco IOS releases.

- CSCso46409

Symptoms: “mbrd_netio_isr” and “crypto_engine_hsp_hipri traceback” log messages are produced.

Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM- VPN/SSL-3.

Workaround: There is no workaround.

- CSCta11223

Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

Conditions: This symptom is observed when the device is running Cisco IOS software and is configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

Workaround: There is no known workaround.

- CSCtb32043

Symptoms: CPUHOG messages may be displayed or the Cisco IOS software might crash when executing no ipv6 multicast-routing in a configuration with more than 20,000 IPv6 multicast-enabled interfaces or subinterfaces.

Conditions: This symptom is observed only rarely when an alternate software path is taken. It is not known what causes this alternate path to be taken.

Workaround: There is no workaround.

- CSCtb55479

Symptoms: A router may crash by the “BGP Router” process.

Conditions: This symptom is observed if the memory is corrupted.

Workaround: There is no workaround.

- CSCtb72734

Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

Workaround: There is no workaround.

- CSCtb74547

Symptoms: A Cisco ASR 1000 DMVPN HUB reloads at the process IPSEC key engine.

Conditions: This symptom is observed when the “Dual DMVPN with Shared Tunnel- Protection” feature is enabled and the interface is shut down and brought up again.

Workaround: There is no workaround.

- CSCtc49086

Symptoms: When configuration changes are performed within a multicast-enabled VRF that cause the PIM register tunnel interface to go down and up again, spurious memory access appears when traffic is sent at the same time.

Conditions: This symptom occurs when traffic is sent when configuration changes are performed.

Workaround: There is no workaround.

- CSCtd23069

Symptoms: A crash occurs because of a SegV exception after configuring the ip virtual-reassembly command.

Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCte27828

Symptoms: Call forward does not work.

Conditions: Topology: call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider.

IP addresses: CUCM10.10.10.3 Cube SUD10.10.10.2 CUBE North192.168.101.10 SBC 192.168.100.5

“Call forward no answer” scenario does not work, but not systematically: sometimes it works, sometimes not.

When the “call forward no answer” fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC doesn’t answer due to this.

Workaround: There is no workaround.

- CSCtf24052

Symptoms: On a Cisco router loaded with Cisco IOS Release 15.0(1)M or Release 15.1(1)T, traffic may not match the ACL configured with a port range inside a class map.

Conditions: This symptom is observed when port range ACE is configured after a few ACEs, as in the following example:

```
Flashcard# show access-lists 101

Extended IP access list 101
 10 permit icmp any any
 20 permit udp any any eq domain
 30 permit udp any eq domain any
 40 permit tcp any any range <start> <end>
 50 permit tcp any range <start> <end> any
<removed>
 220 permit tcp any any range <start> <end>
```

Workaround: Use ACE with a specific port to match the traffic, or use IP source/destination.

- CSCtf32100

Symptoms: Packets are dropped.

Conditions: This symptom is observed with router-destined traffic on an interface with VRF and crypto map configured, when the hardware is Cisco 7200 G2 with VSA.

Workaround: There is no workaround.

- CSCtf71673

Symptoms: A Cisco 10000 series router shows a PRE crash due to memory- corruption with block overrun.

Conditions: This symptom is seen when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

Workaround: There is no workaround.

- CSCtf81249

Symptoms: Memory leaks occur while configuring Cisco IOS commands.

Conditions: This symptom is observed only when configuring from telsh.

Workaround: Use the **end** command specifically to avoid any leaks.

- CSCtg41206

Symptoms: In a Cisco 7200VXR NPE-2 with VSA crypto accelerator enabled and GDOI crypto-map applied to an interface, egress QoS classification is not happening for non-encrypted packets. As the result, these packets end up in class-default and being treated accordingly. Packets/bytes/rate counters in class-default are not counting these packets properly. Encrypted packets are processed correctly.

Conditions: This behavior is observed in all Cisco IOS Releases 12.4(24)T and 15.0(1)M.

Workaround: Disable VSA crypto accelerator with the **no crypto engine slot 0** global configuration command. Switching to software crypto engine may adversely affect router's crypto processing performance, CPU load, and control plane stability.

- CSCtg47129

The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat>

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtg68047

Symptoms: The router reloads.

Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

Workaround: Wait until the tunnels are shut down before issuing the show command.

- CSCtg68208

Symptoms: A router may repeatedly reload when an L2TPv3 xconnect configuration is present and there is no interface configured with an IP address.

Conditions: This symptom has been observed when the **xconnect** command specifies **encapsulation l2tpv3**, and all interfaces on the router are either configured with **no ip address** or **ip address dhcp**.

Workaround: To avoid this problem, ensure there is an interface that is able to reach the L2TPv3 peer and that has an IP address configured.

- CSCtg72652

Symptoms: On Cisco 2900 series routers, the following warning message might display on the console:

```
%ENVMON-1-POWER_WARNING: : Chassis power is not good in the PSU 1
```

Conditions: Under rare conditions, the power supply sometimes sends a false alarm status to the system, even though the system power is working fine.

Workaround: There is no workaround.

- CSCtg73604

Symptom: E1R2 compelled signaling calls fail.

Conditions: This symptom is observed when a call is made using E1R2 compelled signaling.

Workaround: There is no workaround.

- CSCtg84969

Symptoms: The output of **show ip mfib vrf <vrf name> verbose** may show the following line “Platform Flags: NP RETRY RECOVERY HW_ERR” and multicast traffic may not be hardware switched.

Conditions: The symptom is observed on a dual RP Cisco 7600 series router with linecards after multiple reloads or SSO switchovers. When the issue occurs the output of **show ip mfib vrf <vrf name> verbose** on the standby SP will show some lines preceded with “###” where an interface name is expected.

Workaround: There is no workaround.

- CSCtg89555

Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

Conditions: This symptom is observed when configuring an ip address after multicast has been configured on a dot1Q interface.

Workaround: Performing a **shut/no shut** of the interface will fix the problem.

- CSCth01526

Symptoms: MDT interface deactivated and activated after an SSO.

Conditions: After an SSO switchover, the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

Workaround: There is no workaround.

- CSCth01939

Symptoms: IPsec packets are dropped on the router and an error is displayed on the console.

Conditions: This symptom is observed on a Cisco IAD2430 with VPN/GRE tunnel configuration and AES256 encryption.

Workaround: There is no workaround.

- CSCth11006

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

NetMeeting Directory (Lightweight Directory Access Protocol, LDAP) Session Initiation Protocol (Multiple vulnerabilities) H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is posted at <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCth28702

Symptoms: This bug has been filed to enhance the code to follow secure best practices and enhance resiliency of the product.

Conditions: Not applicable.

Workaround: Not applicable.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCth45432

Symptoms: Traffic that is CEF-switched through the router does not exit Async interfaces.

Conditions: This symptom is observed with CEF enabled and in Cisco IOS Release 12.4(20)T and above with MFI.

Workaround: Disable CEF or downgrade to Cisco IOS Release 12.4(15)T before MFI.

- CSCth84233

Symptoms: Router may crash due to Redzone memory block corruption (I/O) when "qos pre-classify" is configured under tunnel interfaces. The packet is overwriting the next block.

Conditions: The trigger for this issue is configuring "qos pre-classify".

Workaround: Remove "qos pre-classify".

- CSCth85294

Symptoms: A PIM neighborship is not established with the remote PE and RP for the MVRFs.

Conditions: This symptom is observed with traffic and after removal and restoration of MVRFs. Traffic does not flow properly since the PIM neighborship is not established with the remote PE and RP for those MVRFs.

Workaround: There is no workaround; however, multiple removals of MDTs could help.

- CSCth87458

Symptoms: Memory leak detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

Conditions: This was experienced during internal protocol robustness testing.

Workaround: Allow SSH connections only from trusted hosts.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2011-2568

has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti01971

Symptoms: The active router crashes during a switchover in a scaled BFD IPv6 setup.

Conditions: The router is configured with a larger number of IPv6 routes with BFD sessions configured. (The test was done with 500 BFD IPv6 sessions.)

Workaround: There is no workaround.

- CSCti18615

Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP being out of sync with the active RP. The A and F flags are missing from the multicast forwarding base entries.

Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, and when the router is in HA mode SSO and is reloaded from the RP.

Workaround: Perform a shut/no shut of the affected interfaces.

- CSCti35326

The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.

The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates the vulnerability is available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-nat>

- CSCti48483

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

NetMeeting Directory (Lightweight Directory Access Protocol, LDAP) Session Initiation Protocol (Multiple vulnerabilities) H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCti48504

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCti64685

Symptoms: User may not be able to configure SLA MPLS configuration.

Conditions: This symptom occurs when the router is booted up and may be random.

Workaround: There is no workaround.

- CSCti81539

Symptoms: Some of the ACLs related to TCP cannot be removed from a router.

Conditions: This symptom is observed while unconfiguring ACLs.

Workaround: Remove the entire ACL, and recreate it again.

- CSCti89976

Symptoms: Standalone AnyConnect 3.0 client does not work with an existing IOS headend.

Conditions: The symptom is observed when AnyConnect 3.0 is used with an existing IOS headend.

Workaround: Use client versions less than or equivalent to 2.5, or use weblaunch.

- CSCti99419

Symptoms: An HWIC-1DSU-T1 card is not recognized after a reload.

Conditions: This symptom is observed on an HWIC-1DSU-T1 card after a reload. It occurs only about 1 to 2 percent of the time.

Workaround: Power-cycle the router.

- CSCtj15798

Symptoms: Some modems in PVDM2-xxDM module are marked as BAD after running clean for few days. The **show modem** command will report a “B” in front of the modem (“B - Modem is marked bad and cannot be used for taking calls”).

Conditions: The symptom is observed with the PVDM2-xxDM module.

Workaround: Reloading the router gives another few days of clean connections before the issue comes back again.

- CSCtj23189

Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.

Conditions: This happens only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with 3 classes: one with 16 kbps, second one with 1 Mbps, and the third one with 99 Mbps.

Workaround: There is no workaround.

- CSCtj33003

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip>

- CSCtj36521

Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj39664

Symptoms: A router that is running Cisco IOS Release 15.1(2)T1 may crash when attempting to configure Zone-Based Firewall.

Conditions: The symptoms are observed when attempting to configure zone-pair. It occurs only with a Cisco 861 router.

- Workaround: There is no workaround.
- CSCtj46670

Symptoms:

IPCP cannot complete after dialer interface is moved out of Standby mode CONFREJ is seen while negotiating IPCP

Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

Workaround: Reload the router.
 - CSCtj47696

Symptoms: A Cisco router supporting HWIC-2CE1T1-PRI WAN module will not process any in/outgoing ISDN calls once the network derived clock is configured (i.e.: “network-clock-participate wic 0”).

Conditions: The symptom is observed on a Cisco 3800/3900 series router with NM-8CE1T1-PRI, HWIC-2CE1T1-PRI or VWIC3-2MFT-T1/E1 running Cisco IOS Release 15.1 (1)T or Release 12.4(24)T4 deriving the clock from the network.

Workaround: Configure “national reserve 0 0 0 0 0 0” under the affected E1 port following by shut/no shut of the E1 port. Complete the workaround by configuring “national reserve 1 1 1 1 1 1” and flapping the port one more time.

If modem calls are not required, “no network-clock-participate” can also be used as a workaround.

Further Problem Description: Problem is not seen on VWIC2-2MFT-T1/E1.
 - CSCtj52077

Symptoms: Policy at subinterface is not accepted with CBWFQ.

Conditions: This symptom is observed when policy is used in Ethernet subinterface.

Workaround: There is no workaround.
 - CSCtj79676

Symptoms: The router crashes sometimes once CEF is enabled.

Conditions: This symptom occurs when CEF is enabled.

Workaround: There is no workaround.
 - CSCtj84234

Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBRed in hardware. This symptom is observed with route-map configuration, as given below:

```
route-map <RM name>
  match ip address <acl>
  set ip next-hop <NH1> <NH2>
```

Workaround: There is no workaround.
 - CSCtj95685

Symptoms: A router configured as a Voice Gateway may crash while processing calls.

Conditions: The symptom is observed with a router configured as a Voice Gateway.

Workaround: There is no workaround.

- CSCtk00181

Symptoms: Password aging with crypto configuration fails.

Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

Workaround: There is no workaround.

- CSCtk01638

Symptoms: Analog endpoint and connection trunk is torn down due to the following Q.850 cause code in SIP BYE request:

Port will show in a S_TRUNK_PEND

show voice call summary | include 0/2/0

0/2/0- - - S_TRUNK_PEND

Conditions: This symptom is observed when the **clear counters** command is invoked. This triggers the gateway to stop sending rtcp events, which causes media inactivity to be activated on the far-end gateway and the connected trunk to be torn down.

Workaround: There is no workaround.

- CSCtk02814

Symptoms: The **show pppoe throttled subinterfaces** command output is truncated, and does not show throttled ATM VC or QinQ subinterfaces during throttling.

Conditions: This symptom occurs when pppoe throttling is configured and active.

Workaround: There is no workaround.

- CSCtk13720

Symptoms: A Cisco router may crash when trying to remove an entry from an extended access-list.

Example:

```
Extended IP access list < NAME >
  10 permit tcp any any ack
  20 permit tcp any any fin
  30 permit tcp any any ack fin
  40 permit tcp any any rst
```

```
Router (config)# ip access-list extended < NAME >
Router (config-ext-nacl)# no 10
```

Conditions: This symptom was first found on a Cisco router running Cisco IOS Release 15.0(1)M4 with extended access-lists and QoS configured. After further testing, we were able to determine that Cisco IOS Release 15.1(3)T did not crash due to this bug.

Router will crash only if we have TCP flags in the ACL.

Workaround: To modify an ACL, follow these steps:

1) Remove ACL filter from the class. For example:

```
class-map match-any c1
  no match access-group name QOS-TCP-OPTIONS
```

2) Modify the ACL:

```
ip access-list extended QOS-TCP-OPTIONS
  no 10
```


3) Re-add the ACL filter in class:

```
class-map match-any c1
  match access-group name QOS-TCP-OPTIONS
```

So basically, *do not* modify ACL if the ACL is configured as a filter under any class. Remove filter first, modify ACL and re-add filter to class.

- CSCtk32975

Symptoms: The system crashes.

Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

Workaround: There is no workaround.

- CSCtk67709

Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

```
ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432- k9.pkg
SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
```

Conditions: This symptom is observed with AnyConnect 3.0.

Workaround: There is no workaround.

- CSCtk67934

Symptoms: A Cisco router is forced to reload after a few days of encryption and decryption while processing high traffic.

Conditions: This symptom is observed when VSA is enabled as a hardware crypto engine used for processing both firewall and encryption/decryption on the same interface.

Workaround: Switch from VSA HW crypto engine to either SW crypto engine or VAM2+ HW crypto engine.

- CSCtk74685

Symptoms: When H225 messages for a call are sent out to the wrong TCP socket by a Cisco IOS gateway, they may sent to a completely different IP than the one that is aware of the call. When this occurs, the new socket gets paired to the call and the H323 stack tries to tear down the H245 socket for a call that is being disconnected. Instead, it erroneously tears down an unrelated calls H225 socket. This causes the unrelated call to drop.

Observed with “debug cch323 all” and “debug ip tcp trans:”

```
13090333: Dec 3 13:18:20.965: //137091/80C6B1F78F31/H323/run_h245_iwf_sm: received
IWF_EV_H245_DISCONNECT while at state IWF_ACTIVE 13090334: Dec 3 13:18:20.965:
//137091/80C6B1F78F31/H323/cch323_send_event_to_h245_connection_sm: Changing to new
event H245_DISCONNECT_EVENT 13090335: Dec 3 13:18:20.965:
//137091/80C6B1F78F31/H323/cch323_h245_connection_sm: state=0, event=4,
ccb=C5E442B8, listen state=2 13090336: Dec 3 13:18:20.965:
//137091/80C6B1F78F31/H323/cch323_h245_connection_sm: H245_CONNECT: Received event
H245_DISCONNECT_EVENT while at H245_NONE state 13090337: Dec 3 13:18:20.965: TCP0:
state was ESTAB -> FINWAIT1 [24696 -> 192.0.2.100(1720)] 13090338: Dec 3 13:18:20.965:
TCP0: sending FIN
```

Conditions: This symptom occurs with all IOS images with the fix for CSCin76666.

The cascade issue noted in this bug is triggered by an event where CM closes down an H225 or H245 TCP socket mid-call. Due to the cascading nature of CSCtk74685, identifying the root call that triggers this socket conflict may be extremely difficult, until the fix for CSCtk74685 is applied.

Workaround: Use one of the following workarounds:

1. Enable call preservation on CM, which does not prevent the socket from getting torn down, but minimizes user impact and does not drop audio on the call.

voice service voip h323 call preserve

System > Service Parameters > (Select Publisher Node) > Cisco CallManager > Advanced > Allow Peer to Preserve H.323 Calls > False > Save

2. Run a Cisco IOS release that does not have the fix for CSCin76666.

3. Change the signaling protocol to SIP.

- CSCtl20509

Symptoms: CME/SRST 4.0 when ATA unregister/ fall back to Cisco Unified CallManager, the virtual POTS dial-peers stay up and calls to ATA do not go out the H323 dial-peer to Cisco Unified CallManager. The calls fail with user busy. This issue affects only ATA. Dial peers of the IP phones behave normally.

Conditions: This symptom occurs when the ATA fallback to the CCM occurs and registers with the CCM. However, The virtual pots dial peer for the ATA are up.

Workaround: Reload the router.

- CSCtl45684

Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

```
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726 ASSERTION
FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
```

Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.

Workaround: There is no workaround.

- CSCtl54975

Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

Conditions: Unknown.

Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl67079

Symptoms: Following error message is seen on Cisco router with HWIC_1GE_SFP inserted:

```
%HWIC_1GE_SFP-3-INTERNAL_ERROR: GigabitEthernet0/0/0 SNMP high capacity counter
register failed
```

Conditions: This symptom is observed during bootup.

Workaround: There is no workaround.

- CSCtl87879

Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

Workaround: There is no workaround.

- CSCtl95752
Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.
Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.
Workaround: There is no workaround.
- CSCtn08208
Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.
Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.
Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.
- CSCtn10922
Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.
Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.
Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.
- CSCtn12119
Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.
Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.
Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.
- CSCtn16855
Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.
Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.
Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.
- CSCtn19496
Symptoms: Packet loss is seen when the service policy is applied on the tunnel interface. The **show hqf interface** command output shows drops in a particular queue with the following:
Scheduler_flags 177
The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.
Conditions: This symptom is observed when the service policy is applied on the tunnel/GRE interface, and when the source of the tunnel interface is the ATM interface(hwic-shdsl).
Workaround: There is no workaround.
Further Problem Description: The above-described symptom is seen only with the SHDSL link.

- CSCtn48744
Symptoms: Memory leaks on OER border router while running PfR-IPSLA configuration.
Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.
Workaround: There is no workaround.
- CSCtn68643
Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.
Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption.

```
ipv6 ospf encryption ipsec spi 500 esp null sha1
123412341234123412341234123412341234123412341234
```


or

```
ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcdabcd
```


Workaround: There is no workaround.
- CSCtn72939
Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.
Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.
Workaround: Configure bridge-group under that xconnect interface.
- CSCtn74673
Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.
Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.
Workaround: There is no workaround other than line card reload.
- CSCto07919
Symptoms: Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
 - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload.
 - ICMPv6 Packet May Cause MPLS-Configured Device to Reload.
 Cisco has released free software updates that address these vulnerabilities.
Workarounds that mitigate these vulnerabilities are available.
This advisory is posted at:
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>
- CSCto08135
Symptoms: When a deny statement is added as the first ACL, the message gets dropped.
Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.
Workaround: Turn off the VSA, and go back to software encryption.

- CSCto08754
Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.
Conditions: This symptom occurs when the crypto VTI interface becomes wedged.
Workaround: There is no workaround.
- CSCto13254
Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error: Hash verification failed for file <temp location of profile>
Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.
Workaround: Remove the profile from the Cisco IOS headend.
- CSCto14435
Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.
Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.
Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.
- CSCto41173
Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.
Conditions: This symptom is observed with a platform that acts as an H323 gateway and runs Cisco IOS Release 15.1(3)T.
Workaround: Revert to Cisco IOS Release 12.4(20)T.
- CSCto53332
Symptoms: A router configured for IPSEC accounting may display the following error message:
`%AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed`
This does not seem to result in any impact apart from intermittently lost accounting messages.
Conditions: This symptom occurs when ipsec accounting is active.
Workaround: There is no workaround.
- CSCto55643
Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.
Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.
Workaround: There is no workaround. Ensure that mls rate limits are properly configured.
Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.
- CSCto55983
Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

Workaround: There is no workaround.

- CSCto63268

Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

Workaround: Remove the EVM or disable DSP sharing.

- CSCto63954

Symptoms: A router with GETVPN configurations is continuously crashing.

Conditions: This symptom is seen with GETVPN related configurations with fail-close feature activated.

Workaround: There is no workaround.

- CSCto68554

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>.

- CSCto72480

Symptoms: The output of the **show mfib linecard** command shows that line cards are in “sync fail” state.

Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

Workaround: If this issue is seen, using the **clear mfib linecard slot** command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto72927

Symptoms: Configuring an event manager policy may cause a cat4k to hang.

Conditions: Configuring a TCL policy and copying that policy to the device.

Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.7/3.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C> No CVE ID

has been assigned to this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCto86833

Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DN's with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

Workaround: If possible, reduce the number of voice ports automatically generated by the number DN's and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- CSCto88686

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCto93837

Symptoms: Cisco IOS may experience a memory leak when parsing certain responses to an outgoing SUBSCRIBE.

Conditions: Cisco IOS is configured to process SIP messages.

Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2011-4019 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq05004

Symptoms: A dialer loses its IP address sporadically. The **show interface atm x** will record output drops during the issue. ATM0 is up, line protocol is up:

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 31956 << Incrementing during the issue

The **show interface queueing atm0.1** hidden command will show as follows:

```
Interface ATM0 VC 8/35 Queueing strategy: fifo Output queue 40/40, 31956 drops per VC
<< Incrementing during the issue
```

During the issue, if “debug ppp negotiation” is on, we will see the following:

```
PPP: Missed 5 keepalives, taking LCP down PPP DISC: Missed too many keepalives
```

There will be no ATM (physical interface) flap in this case (during the issue).

A shut/no shut on the ATM interface does not help.

Conditions: No conditions so far. The behavior is sporadic.

Workaround: Reload.

- CSCtq05636

Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg. For example:

Received: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0

Sent: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0

In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq07413

Symptoms: A hardware crypto engine may fail to decrypt packets. An “invalid parameter” error is seen after decryption. Software encryption works fine.

Conditions: This symptom is observed in Cisco IOS Release 12.4.15T6.

Workaround: Use software encryption.

- CSCtq09899

Symptoms: The VXML gateway crashes.

Conditions: This symptom occurs during the load test, when the **show mrccp client session active** is used.

Workaround: There is no workaround.

- CSCtq10684

Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

Conditions: This symptom occurs when tunnel flap is observed before the crash.

Workaround: A possible workaround is to reload the box.

- CSCtq12007

Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less severe; you may see one every other packet drop, until the next rekey or tunnel reset.

Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq15247

Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

For example:

```
LAC1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
LAC1(config)# interface virtual-ppp1
LAC1(config-if)# no pseudowire
LAC1(config-if)# exit
LAC1(config)# no interface virtual-ppp1
```

- CSCtq24733

Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.

Conditions: The symptom is observed with MRCP is enabled.

Workaround: There is no workaround.

- CSCtq27180

Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.

Conditions: This symptom is observed only on IOS internal releases.

Workaround: There is no workaround.

Further Problem Description: The following LOG messages and errors are found:

```
Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed -Traceback=
604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z Mar
30 01:27:38.447: %LICENSE-2-VLS_ERROR: 'VLSsetInstallLicenseStorage' failed with an
error - rc = 136 - 'Error[136]: Specified license store doesn't exists.' -Traceback=
604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z
```

- CSCtq28732

Symptoms: Memory leak observed when device configured with the **parameter-map type inspect global** command.

Conditions: Device is configured with the **parameter-map type inspect global** command.

See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>

Workaround: None.

Further Problem Description: The following software table provides the first fixed release for each affected train for this specific Cisco ID.

```
+-----+ | Release | First Fixed Release for this | | Cisco bug ID |
+-----+-----+ | 15.0 Releases | +-----+-----+ |
No affected 15.0 releases | +-----+-----+ | 15.1 Releases |
+-----+-----+ | 15.1M | 15.1(4)M2 | | 15.1MR | Not Vulnerable | | 15.1S |
Not Vulnerable | | 15.1SG | Not Vulnerable | | 15.1T | 15.1(2)T4, 15.1(3)T | | 15.1EY | Not Vulnerable
| | 15.1GC | Vulnerable | | 15.1MWR | Not Vulnerable | | 15.1XB | Vulnerable |
+-----+-----+ | 15.2 Releases | +-----+-----+ |
No affected 15.2 releases | +-----+-----+ |
```

- CSCtq30875

Symptoms: A Cisco ISR G1 will display “March 11, 2011” when the **show clock** command is entered. This will effect functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

Workaround: The clock can be set manually via CLI.

- CSCtq36153

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfbw>

- CSCtq39406

Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

Conditions: This symptom occurs when you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM.

Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- CSCtq47428

Symptoms: A Cisco router acting as an SRST may unexpectedly reload due to a bus error.

Conditions: This symptom is observed with phones registered to the SRST.

Workaround: There is no workaround.

- CSCtq56727

Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash.

The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP, and other processes.

“sh proc mem sorted” shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

Conditions: This symptom occurs when the SIP trunk in Unified Communications Manager pointing to the gateway is configured with a DTMF signaling type of “no preference” and the SIP gateway is configured with DTMF relay as sip- kpml.

Workaround: There are two workarounds:

1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”

Recovery: In order to recover from the crash, you must reload the gateway router.

- CSCtq61850

Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

Workaround: There is no workaround.

- CSCtq64951

Symptoms: The following message is displayed:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality
with securityk9 technology package license.
```

The **show platform cerm** command output shows all tunnels in use by SSLVPN.

```
Number of tunnels 225 ... SSLVPN D D 225 N/A
```

The **show webvpn session context all** command output shows no or very few active sessions.

```
WebVPN context name: SSL_Context
```

```
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
```

Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq75008

Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

Conditions:

- The Cisco 7206 VXR works as a server for L2TP over IPsec.
- Encryption is done using C7200-VSA.
- More than two clients are connected.

If client sessions are kept up for about a day, the router crashes.

Workaround: There is no workaround.

- CSCtq83629

Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

Workaround: Line card reload is required to resolve the problem.

- CSCtq86500

Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

Workaround: Disable VSA and use software encryption.

- CSCtq86515

Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq91176

Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtq92940

Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtr04829

Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

Conditions: This symptom occurs when the hardware address is zero.

Workaround: There is no workaround.

- CSCtr11620

Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

Conditions: This symptom is observed when a Cisco 2911 is used.

Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr29338

Symptoms: A router crashes.

Conditions: The symptom is observed after an “%ISDN-6-DISCONNECT” message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

Workaround: There is no workaround.

- CSCtr44686

Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
  class type inspect smtp SMTP_L7_C1
    reset
policy-map type inspect smtp SMTP_L7_P2
  class type inspect smtp SMTP_L7_C2A
    reset
  class type inspect smtp SMTP_L7_C2B
    reset
```

Conditions: The symptom is observed with the above maps.

Workaround: Replace “reset” with “log”.

- CSCtr46123

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

- CSCtr49064

The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh>

- CSCtr51926

Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

Conditions: The symptom is observed when a service-policy is applied on the main interface.

Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y
  ipv6 enable
```

Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z
  no ipv6 address
  ipv6 address ...
```

- CSCtr54269

Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr86437

Symptoms: NAT-PT function does not work properly after an interface flap occurs.

Conditions: The symptom is observed when you configure NAT-PT on the router.

Workaround: Reconfigure “ipv6 nat prefix.”

- CSCtr91106

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

- CSCtr97640

Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

Conditions: None.

Workaround: None—Physically securing the router is important.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.9/1.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C> CVE ID CVE-2011-3289

has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts28315

Symptoms: A DHCP PD request does not accept a specific server.

Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

<http://tools.ietf.org/html/rfc3633#section-10>

A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

Workaround: There is no workaround.

- CSCts33952

Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

Workaround: There is no workaround.

- CSCts59014

Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

Workaround: There is no workaround.

- CSCts76410

Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

Conditions: The symptom is observed during a rekey, when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCtt20215

Symptoms: VWIC3 E1 cas connect to PBX, controller down after reload

Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

Workaround: Need to unplug/plug the cable, or reset link from PBX side, controller will come up.

Resolved Caveats—Cisco IOS Release 15.1(1)T3

Cisco IOS Release 15.1(1)T3 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T3 but may be open in previous Cisco IOS releases.

- CSCsk65515
 Symptoms: Spurious or misaligned memory access can be seen at atm_nvgen_static_map.
 Conditions: The symptoms can be observed when an SVC is configured on an ATM interface and when executing the command **show running- config**.
 Workaround: There is no workaround.
- CSCso33003
 Symptoms: If a child policy is attached to a parent policy twice, the router will reload if child policy configuration is removed.
 Conditions: The parent policy needs to be attached to target interface.
 Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.
- CSCta26520
 Symptoms: The following traceback is seen:

```
%IDBINDEX_SYNC-3-IDBINDEX_LINK: Driver for IDB type 0 changed the Identity of
interface "Tunnell" without deleting the old Identity first.
```

 Conditions: This symptom is observed when numerous tunnel interfaces are rapidly added and removed.
 Workaround: There is no workaround
- CSCtb07984
 Symptoms: A Cisco ASR router acting as LNS fails to apply D2 QoS on first few sessions after every new reboot and configures the D2 QoS on all subsequent sessions.
 Conditions: The symptom is observed when multiple routes exist on an LNS router to reach LAC router. PPPoX sessions are brought on LNS with D2 QoS model after new reboot of router.
 Workaround 1: LNS router configures D2 QoS on all subsequent sessions in Cisco IOS Release 12.2XND images.
 Workaround 2: In Cisco IOS Release 12.2XNE images, LNS router should have a single route to reach LAC router.
 Workaround 3: Wait until CEF is converged before bringing up a second session on the LNS router.
- CSCtc67457
 Symptom: Cisco ASR1000-RP2 crash is seen with the IKMP process.
 Conditions: This symptom occurs with GetVPN group member configurations with VRF-lite.
 Workaround: There is no workaround.

- CSCtd10712

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCte18124

Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024”.

Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.

Workaround: Create ATM PVC without “atm vc-per-vp 1024”.

- CSCte78406

Symptoms: The following error message is logged at the new standby RP when PTA sessions are established:

```
%COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-Access2.1
linked to wrong idb Virtual-Access2.1
```

Conditions: The symptom is observed when PTA sessions are established, then an RP switchover is performed. After both RPs sync up, flap the sessions. The error messages are logged at the new standby RP.

Workaround: There is no workaround.

- CSCtf26639

Symptoms: A router crashes when turning on WAAS, adding a couple of specific class maps, and then turning off WAAS.

Conditions: This is a corner case that is seen only when a specific type of filter is used with two or more classes; for example, for a WAAS class of the following type:

```
class-map type waas DT-40 match tcp source ip 192.168.1.116 dest port 10040 10049
class-map type waas DT-50 match tcp source ip 192.168.1.116 dest ip 192.168.101.117
port 10050 10059

policy-map type waas waas_global class DT-40 insert-before waas-default optimize tfo
application DT-40 class DT-50 insert-before waas-default optimize tfo application
DT-50 end
```

The router will crash with such a configuration. Here, we have all TCP filters with same source IP address. This is the special condition.

Workaround: There is no workaround.

- CSCtf36402

Symptoms: A Cisco router crashes when the user telnets and Transmission Control Block is cleared for that session before entering the password.

Conditions: This symptom is observed when aaa authentication protocol is set to TACACS.

Workaround: Do not clear the Transmission Control Block for a session before entering the password.

- CSCtf56107

Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

Conditions: The symptom is observed when an unknown notify message is received.

Workaround: There is no workaround.

- CSCth03022

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCth20696

Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

Conditions: The symptom is observed with Cisco IOS Release 12.4(25c).

Workaround: There is no workaround.

- CSCth35515

Symptoms: Linecard crash could occur on an SSO when a router runs MPLS.

Conditions: This symptom may occur when multiple back-to-back switchovers occur.

Workaround: There is no workaround.

- CSCth40506

Symptom: A Cisco voice gateway does not have its GigabitEthernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

```
-- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
```

Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

```
-- .May 4 17:49:29.120 GMT=+1: ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry:
Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
```

The call, however, is not cleared from the PRI.

- CSCth46888
Symptoms: When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.
Conditions: The symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.
Workaround: There is no workaround.
- CSCth57478
Symptoms: When configuring SIP digest authentication, user names with more than 25 characters are truncated in the running config and cause the password component to be corrupted. This error is saved through to startup configuration, causing the authentication to be lost on reboot.
Conditions: This symptom is observed with a normal dial-peer configuration on a POTS dial-peer running Cisco IOS Release 15.1(1)T.
Workaround: There is no workaround.
- CSCth69364
Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.
Cisco has released free software updates that address this vulnerability.
This advisory is posted at
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw>.
- CSCth93218
Symptoms: The error message "%OER_BR-4-WARNING: No sequence available" displays on PfR BR.
Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.
Workaround: There is no workaround.
- CSCth94814
Symptoms: Crash is seen in static route component.
Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.
Workaround: There is no workaround.
- CSCti05663
Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.
Conditions: The symptom is observed in the case of an numbered relay.
Workaround: There is no workaround.
- CSCti07805
Symptoms: Router reloads @sipSPIUpdSrtpSession.
Conditions: This symptom is observed during Hold/Resume on a basic SRTP call with Cisco IOS Release 15.1(2.3)T.
Workaround: There is no workaround.

- CSCti39902

Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

Conditions: This symptom is observed when RRI is configured on the UUT .

Workaround: There is no workaround.

- CSCti50607

Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

Workaround: There is no workaround.

- CSCti51145

Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

Conditions: This symptom is observed when ALL of the following conditions are met:

- The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”
- It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload
- When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages
- Both peers must be multisession-capable
- “Transport multi-session” must not be configured on either device, or enabled by default on either device
- “Graceful restart” must not be configured.

Workarounds:

1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS 12.2(33)SB-based releases if the 12.2(33)SB router is the one not reloading.

- CSCti61949

Symptoms: Unexpected reload with a "SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header" and "chunk name is BGP (3) update" messages.

Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti67102

Symptoms: Tunnel disables due to recursive routing loop in RIB.

Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

Workaround: There is no workaround.

- CSCti67447

Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

Conditions: The symptom is observed under the following conditions:

1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2
2. Enable MPLS LDP GR.

Workaround: There is no workaround.

- CSCti68721

Symptoms: The output of **show performance monitor history interval <all | given #>** will appear to have an extra column part way through the output.

Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

Workaround: If the symptom occurs, repeat the command.

- CSCti71071

Symptoms: The command **show policy-map multipoint** does not show any output on a hub, configured with a per-tunnel-QoS policy on its tunnel interface. The command is also not displayed in the parser options upon issuing **show policy-map ?**.

Conditions: The symptom is observed with the **show policy-map multipoint** command.

Workaround: There is no workaround.

- CSCti75666

Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.

Workaround: Convert H.323 leg to SIP.

- CSCti79848

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>.

- CSCti84762

Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

Conditions: This is seen with peer flaps or route churn and with an interface flap.

Workaround: Do a hard reset of the stuck peers.

- CSCti85446

Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

Conditions: The symptom is observed with the following conditions:

1. Configure a nexthop static route with permanent keyword
2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface)
3. Change the configuration in such a way that nexthop is reachable
4. Configure a new static route through the same nexthop IP address used in step 1.

Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti87502

Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.

Conditions: This symptom is observed when attempting to launch CP Express.

Workaround: A power cycle fixes the issue temporarily.

- CSCti90602

Symptoms: The PPTP connection is not established when “ip nat outside” is configured on the NAT router. The NAT router is between the client and the server.

Conditions: This symptom is observed only with the PPTP connection; all other traffic works fine.

Workaround: There is no workaround.

- CSCti96028

Symptoms: A build failure is seen due to the fix committed using CSCti67511 (“Borghetti DSL PHY Firmware upgrade through usb flash”).

Conditions: This symptom is observed when building Cisco 180x platform IOS images.

Workaround: There is no workaround.

- CSCti98219

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCtj05903

Symptoms: Some virtual access interfaces are not created for VT on reload.

Conditions: This symptom occurs on scaled sessions.

Workaround: There is no workaround.

- CSCtj08533

Symptoms: QoS classification fails on egress PE if the route is learned via BGP.

Conditions: The symptom is observed when there are redundant paths to the CPE.

Workaround: Use only one path between PE and CPE.

- CSCtj20545

Symptoms: When a host behind a ZBF implementation is disconnecting ungracefully and loses the TCP connection information, TCP keepalive sessions will only be terminated on the other endpoint after the TCP keepalive times out. This is because the RST from the host, in response to the keepalive from other endpoint, is out-of-order and gets dropped by the ZBF.

Conditions: The symptom is observed when you have TCP connections using keepalive (keepalive with both sequence number and acknowledgment number one less than expected for a session) going over a ZBF implementation.

Workaround: Shorten the keepalive timeout on the other endpoint.

- CSCtj21696

Symptoms: The virtual access interface remains down/down after an upgrade and reload.

Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv NAME: "chassis", DESCR: "2801 chassis" PID: CISCO2801 , VID: V04 ,
SN: FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet" PID: CISCO2801
, VID: V04 , SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard" PID:
VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch" PID: HWIC-4ESW , VID: V01 , SN:
FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire" PID:
WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMMII DSP SIMM with one DSP with half channel capacity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB
```

Workaround: Do a shut/no shut on the serial interface.

- CSCtj24453

Symptoms: The following traceback is observed when **clear ip bgp *** is entered:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP Scanner", ipl= 0, pid= 549
with call stack 0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
0x403A4E84:bgp_scanner(0x403a4c50)+0x234
```

Conditions: This symptom is rarely observed, but it can be seen when **clear ip bgp *** is entered with a lot of routes and route-map-cache entries.

```
Router# show ip bgp sum
```

```
BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
main routing table version 1228001 604000 network entries using 106304000 bytes of
memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
cache entries using 4565920 bytes of memory
```

The **clear ip bgp *** command is not a very common operation in production network.

Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the symptom will not be observed.

- CSCtj28747

Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an “Exit Mismatch” message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj30155

Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

- Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
- ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>

- CSCtj35792

Symptoms: The onboard GE on a Cisco 3900 (driver PQ3_TSEC) with “media-type sfp” goes to 1000/HD when it is connected by fiber to a gig port that is not doing autonegotiation.

Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation. The Cisco 3945-E does not have this problem.

Workaround: Configure autonegotiation on the other side, if possible.

Further Problem Description: It is impossible to disable autonegotiation on the Cisco 3900 because of CSCth72105.

- CSCtj41194

Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6>.

- CSCtj47736

Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

Workaround: There is no workaround.

- CSCtj48629

Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtj48913

Symptoms: Track does not recognize when an HTTP IP SLA probe’s status changes to OK.

Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

Workaround: There is no workaround.

- CSCtj53363

Symptoms: Router hangs and console does not respond indefinitely.

Conditions: The symptom is observed with the following conditions:

- AIM-VPN in ISR + ZBFW; or
- A Cisco 2811/2821 Onboard VPN + ZBFW
- Once traffic starts, router hangs within minutes.

Workaround: If running a Cisco 2811/2821, use sw crypto + ZBFW.

Alternate Workaround: If running with a Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj69886

Symptoms: NTP multicast over multiple hops.

Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

Workaround: There is no workaround.

- CSCtj77477

Symptom: High delay in priority queue when using CBWFQ/LLQ. For example:

```
EFM rate 2304 kbps
```

```
888E Average delay: 42ms 888E Max delay: 63ms HWIC-4SHDSL-E Average delay: 216ms
HWIC-4SHDSL-E Max delay: 361ms
```

Conditions: The symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface.

For example:

```
EFM rate 2304 kbps
```

```
policy-map CHILD class voice priority percent 25 class business bandwidth percent 50
policy-map PARENT class class-default shape average 2100000 8400 0 service-policy
CHILD
```

- CSCtj78210

Symptoms: One-way audio. Moves from one port to another when the router is rebooted.

Conditions: The symptom is observed when using multiple “session protocol multicast,” “connection trunk” configurations for LMR, E&M Immediate, and/or other multicast applications, such as the conditions where this was first detected, in a Radio over IP solution. Only affects PVDM3.

Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

For example, configure:

```
voice-card 0 (1... 2... etc...) dspfarm dsp service dspfarm
dspfarm profile x conf max sessions xx << use the maximum max partic << use the maximum
associate app sccp no shutdown
dspfarm profile x2 conf max sessions xx << use the maximum max partic << use the
maximum associate app sccp no shutdown
dspfarm profile x3 conf max sessions xx << use maximum (if allowed) max partic << use
the maximum (if allowed) associate app sccp no shutdown
dspfarm profile x conf shutdown no dspfarm profile x conf
```

The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- CSCtj81533

Symptoms: The following error messages is seen:

```
np_vsmgr_modify_connection: invalid service id 11 passed
```

No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

Workaround: There is no workaround.

- CSCtj82292

Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

Conditions: This issue occurs when summary address is advertised as follows:

```
ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
```

Workaround: There is no workaround.

- CSCtj84901

Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

1. Service Ready Engine modules (ISM and SM SRE)
2. Etherswitch modules (SM and EHWIC)

If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj87180

Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of "SSS Manager Disconnected Session".

Conditions: The symptom is observed when the LAC router receives an incorrect "Error code(9) : Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID" message from the multihop peer.

Workaround: There is no workaround.

- CSCtj89941

Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

Conditions: Testbed setup:

1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured
2. Use IXIA to generate 1Gbps traffic
3. Wait until all the SAs have been established and traffic is stable
4. Use CLI **clear crypto session** on EzVPN simulator.

Workaround: There is no workaround.

- CSCtj94617

Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

Conditions: This symptom is observed when issuing the **show running** command.

Workaround: There is no workaround.

Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

- CSCtj96915

Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

Conditions: Unknown. See Further Problem Description below.

Workaround: There is no workaround. Only a power cycle can remove the symptom.

Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtk02647

Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

Workaround: There is no workaround.

- CSCtk12608

Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, Release 15.1 (2)T and Release 15.1(01)S and with the following configurations:

```
Router 1: interface Ethernet0/0 ip address 10.0.12.1 255.255.255.0 !
interface Ethernet1/0 ip address 10.0.120.1 255.255.255.0 ! router bgp 100 no
synchronization bgp log-neighbor-changes neighbor 172.16.0.1 remote-as 200 neighbor
172.16.0.1 ebgp-multihop 255 no auto-summary !

ip route 0.0.0.0 0.0.0.0 10.10.200.1 ip route 172.16.0.1 255.255.255.255 10.0.12.2 ip
route 172.16.0.1 255.255.255.255 10.0.120.2

Router 2: interface Loopback200 ip address 10.10.200.1 255.255.255.0 ! interface
Loopback201 ip address 172.16.0.1 255.255.255.0 ! interface Ethernet0/0 ip address
10.0.12.2 255.255.255.0 !

interface Ethernet1/0 ip address 10.0.120.2 255.255.255.0 ! router bgp 200 no
synchronization bgp log-neighbor-changes network 10.10.200.0 neighbor 10.0.12.1
remote-as 100 neighbor 10.0.12.1 update-source Loopback201 no auto-summary ! ip route
0.0.0.0 0.0.0.0 10.0.12.1 !
```

Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes.”

- CSCtk12681

Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk47891

Symptoms: Traffic might be blackholed when LC is reset, if Fast Reroute (FRR) is in use.

Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

Workaround: There is no workaround.

- CSCtk53130

Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

Incompatible with ipv6 command on Vp1 - command rejected.

Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

Workaround: There is no workaround.

- CSCtk53534

Symptoms: Router crashes.

Conditions: The symptom is observed with some combination of zone-based firewall and policy configuration and with IPv6 traffic.

Workaround: Disable global parameter-map.

- CSCtk56570

Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.

Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

Workaround: Disable media transcoder-high-density.

- CSCtk62247

Symptoms: IKEv2 session fails to come up with RSA sign authentication.

Conditions: The symptom is observed with a hierarchical CA server structure.

Workaround: Use non-hierarchical CA servers.

- CSCtk67073

The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla>.

- CSCtk68647

Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk74660

Symptoms: The Network Time Protocol (NTP) tries to re-sync after the server clock changes its time and after the NTP falls back to the local clock.

Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

Workaround: There is no workaround.

- CSCtk84116

Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

Workaround: There is no workaround.

- CSCtk95992

Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

Workaround: Configure the command **dls w udp-disable**.

Further Problem Description: This symptom occurs in the following (and later) releases:

Cisco IOS Release 12.4(15)T14, Release 12.4(24)T4, Release 15.0(1)M3, Release 15.1(1)S, Release 15.1(2)T, Release 12.2(33)SX14, and Release 12.2(33)SX14a.

- CSCtl00467

Symptoms: A Cisco router crashes.

Conditions: This symptom is observed when call monitoring is enabled and the “conference call” feature is used.

Workaround: There is no workaround.

- CSCtl04285

Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

Conditions: The symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are Cisco IOS Release 12.2(33)SRE, Release 15.0M, and 12.2(33)XNE and later releases.

Workaround: There is no workaround.

- CSCtl05684

Symptoms: Xauth user information remains in “show crypto session summary” output.

Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different username during P1 rekey.

Workaround: Use save-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl08014

Symptoms: Router crashes with memory corruption symptoms.

Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

Workaround: There is no workaround.

- CSCtl21695

Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million. **Debug vpdn l2x ev/er** shows:

```
PPTP ____:____: TCP connect reqd from 0.0.0.0:49257 PPTP ____:____: PPTP,
no cc in l2x
```

Conditions: This symptom occurs when LNS is configured for PPTP aggregation and over one millions tunnels have been accepted (on VPDN level).

Workaround: Reload LNS.

- CSCtl47666

Symptom: Intermittent call drops for CME SNR calls that go to voicemail.

Conditions: This symptom is observed on a Cisco IP phone with SNR configured. When the “no answer” timer is reached, the call will intermittently drop instead of going to voicemail.

Workaround: There is no workaround.

- CSCtl57055

Symptoms: A router may unexpectedly reload when the rttMonStatsTotalsEntry MIB is polled by SNMP.

Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release, is configured for SNMP polling, and when the rttMonStatsTotalsEntry is polled with an IP SLA probe configured.

Workaround: Configure NMS to stop polling the rttMonStatsTotalsEntry or create a view and block the MIB on the router.

Alternate Workaround: Since the issue affects only Cisco IOS 15.1T releases, use a Cisco IOS Release 15.0(1)M or earlier rebuild.

- CSCtl71478

Symptoms: In an HA system, the following error message is displayed on the standby RP and LC:

“OCE-DFC4-3-GENERAL: MPLS lookup unexpected”

Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

Workaround: There is no workaround.

- CSCtl73914

Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

Conditions: The symptom is observed if the P-Associated-URI of the 200 Ok response contains any special characters (!*.) in Tel URI Parsing.

Workaround: There is no workaround.

- CSCtl77735

Symptoms: Saving a configuration to NVRAM may fail.

Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

Workaround: Erasing the startup configuration and saving again may recover the configuration.

- CSCtl98132

Symptoms: XDR CPU hog may cause system crash.

Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

Workaround: There is no workaround.

Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtl98270

Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

Conditions: The symptom is observed in Cisco IOS Release 15.1(2)T2 and later releases.

Workaround: Execute a shut/no shut to fix the issue.

- CSCtn26785

Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

```
3845#sh int atm 1/0 stat ATM1/0 Switching path Pkts In Chars In Pkts Out Chars Out
Processor 98170 10995040 1 68 Route cache 0 0 98170 10995040 Total 98170 10995040
98171 10995108 3845#
```

```
3845#sh cef int atm 1/0 ATM1/0 is up (if_number 5) Corresponding hwidb fast_if_number
5 Corresponding hwidb firstsw->if_number 5 Internet address is 64.65.248.174/30 ICMP
redirects are never sent Per packet load-sharing is disabled IP unicast RPF check is
disabled Input features: Ingress-NetFlow Output features: Post-Ingress-NetFlow IP
policy routing is disabled BGP based policy accounting on input is disabled BGP based
policy accounting on output is disabled Hardware idb is ATM1/0 Fast switching type 9,
interface type 138 IP CEF switching enabled IP CEF switching turbo vector IP prefix
lookup IPv4 mtrie 8-8-8-8 optimized Input fast flags 0x0, Output fast flags 0x0
ifindex 5(5) Slot Slot unit 0 VC -1 IP MTU 4470 3845#
```

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn27599

Symptoms: The OIR of NM-1T3/E3 line card crashes the router.

Conditions: This symptom is observed only on the Cisco 3945 router.

Workaround: There is no workaround.

- CSCtn51740

Symptoms: Memory leak is seen in EzVPN process.

Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

Workaround: There is no workaround.

- CSCtn77154

Symptoms: The Stateful Inspection Feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets being punted to the CPU. This causes overall performance degradation.

Conditions: This symptom is observed when two outside NAT interfaces are configured and “no ip nat service nbar” is configured on the interface.

Workaround: Configure “ip nbar protocol discovery” on the interface.

- CSCtn87012

Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

Workaround: Pick up the phone during the ringing OFF cycle.

- CSCto23807

Symptoms: A Cisco device crashes when trying to transfer a call.

Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T2.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(1)T2

Cisco IOS Release 15.1(1)T2 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T2 but may be open in previous Cisco IOS releases.

- CSCso02147

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCsu95339

Symptoms: Output from the **show idmgr session** command displays a corrupted service name.

Conditions: Enter the **show idmgr session** command.

Workaround: There is no workaround.

- CSCsz69148

Symptoms: When running an Embedded Syslog Manager (ESM) TCL script to filter logs on a Cisco ASR 1000 Series Aggregation Services router, memory leaks in IOSD ipc task and ESM Logger occur.

Conditions: The symptom is observed with RP1 and RP2. Any feature which uses heavy logging (for example, audit logging for firewall features) will encounter this issue readily (the trigger is the rate of logging rather than the volume of log messages).

Workaround: There is no workaround.

Further Problem Description: The IOSD ipc task and ESM logger consume more and more memory until there is no more free memory available on the router. You can track the memory consumption with the **show processor memory sort** command and monitor the amount of memory the IOSD ipc task and ESM logger consume over time.

An example configuration:

```
logging buffered filtered
logging filter harddisk:ESMscript.tcl
```

- CSCta15808

Symptoms: Router crashes while printing traceback.

Conditions: The symptom is observed while printing traceback.

Workaround: There is no workaround.

- CSCta53372

Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

Workaround: Reset the RRI session.

- CSCtb55576

Symptoms: When an HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

Workaround: There is no workaround.

- CSCtc33679

Symptoms: Routes are not being controlled properly when PIRO is used.

Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

Workaround: There is no workaround.

- CSCtc55897

Symptoms: R2 will not advertise the routes.

Conditions: The symptom is observed under the following conditions:

1. R2 has two IBDG neighbors in the same update-group one neighbor with 4BAS and the other with 2BAS capability.
2. The locally originated routes or routes without any AS_PATH will not be advertised to this kind of group.

Workaround: Try to make the 2BAS and 4BAS neighbors fall into different update-groups by configuring dummy route-maps.

- CSCtd39579

Symptoms: A router crashes when we try to remove service-policy/waas from an interface.

Conditions: Traffic should be hitting the interface, CPU utilization should be high, and NAT should be applied on the interface as well.

Workaround:

1. Remove NAT from the interface.
2. Remove the service policy.
3. Re-apply NAT.

- CSCtd59027
Symptoms: The device crashes due to a bus error.
Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.
Workaround: There is no workaround.
- CSCte62190
Symptoms: A router crashes when the RSA key is generated with redundancy option and then the RSA key pair is deleted using the **crypto pki zeroize** command. All other possible triggers are not known at this time.
Conditions: Device running IOS and crypto.
Workaround: There is no workaround.
- CSCte64544
Symptoms: Calls fail following hook flash on a T1-CAS circuit.
Conditions: The symptom is observed following outbound calls over a T1-CAS E&M, and after a hookflash.
Workaround 1: Reorder circuits in CUCM RG.
Workaround 2: Perform a shut/no shut on the T1-CAS controller.
- CSCte92581
Symptoms: A VRF becomes stuck during deletion in a rear condition (not something that is seen every time).
Conditions: This symptom is observed when the **no ip vrf** command is entered.
Workaround: There is no workaround.
Further Problem Description: The stuck VRF cannot be reused.
- CSCte94301
Symptoms: IPv6 PBR is not applied to locally-originated ping packets.
Conditions: This symptom occurs when IPv6 PBR is configured for application to locally-originated ping packets.
Workaround: There is no workaround.
- CSCte98702
Symptoms: When using NAT, “%SYS-3-INVMEMINT and %SYS-2-MALLOCFAIL” are printed to the console and no traffic passes.
Conditions: The symptom is observed when NAT is configured.
Workaround: There is no workaround.
- CSCtf34720
Symptoms: DR will not send a periodic join for an SSM group with a “static- group” configuration on the RPF interface. This will result in the S,G states expiring in the upstream routers and may result in traffic loss.
Conditions: The symptom is observed when the static-group join is configured on the RPF interfaces and the output interface list of the mroute is NULL.
Workaround: Add a local join by using **ip igmp join-group** for the same group and source, so that it adds a local interested receiver and sends a periodic join upstream.

- CSCtf54561

Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf vrf-name** command is issued.

Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

Workaround: Command should not be issued when many topology changes occur on interface flaps.

- CSCtg25798

Symptoms: The issue is associated with the two labels imposition for the next-hop address. If there is no label bind for the destination prefix and in order to reach next-hop address the router imposes two labels, only one label is imposed for the final prefix.

Conditions: The symptom occurs when all of the following conditions are met:

1. The prefix does not have a label bind (BGP prefixes for example).
2. There is a static route for the next-hop address pointing to the tunnel only.
3. The router imposes two labels for the next-hop address.

Workaround: There are three potential workarounds:

1. Explicit next hop avoiding recursive research: "ip route 192.168.4.4 255.255.255.255 Tu1 192.168.4.4" (i.e.: breaking rule 2).
2. Use "neighbor 192.168.1.1 send-label" on both PEs (i.e.: breaking rule 1).
3. Use "mpls traffic-eng signaling interpret explicit-null verbatim" on P (i.e.: breaking rule 3).

Further Problem Description: In the following example 192.168.200.200 is the final destination. There is no label bind for this prefix and it is recursive to 192.168.100.100:

```
PE1# show mp ld bin 192.168.200.200 32
lib entry: 192.168.200.200/32, rev 35
      local binding:  label: 31
PE1# show ip route 192.168.200.200
Routing entry for 192.168.200.200/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
    * 192.168.100.100
      Route metric is 0, traffic share count is 1
```

The next-hop 192.168.100.100 has a static route pointing to the tunnel and is double tagged:

```
PE1# show ip route 192.168.100.100
Routing entry for 192.168.100.100/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
    * directly connected, via Tunnel10
      Route metric is 0, traffic share count is 1
PE1# show ip cef 192.168.100.100
192.168.100.100/32
  attached to Tunnel10 label 26
PE1# show mp ld bin 192.168.100.100 32
lib entry: 192.168.100.100/32, rev 30
      local binding:  label: 29
```

```
remote binding: lsr: 192.168.2.2:0, label: 26
remote binding: lsr: 192.168.4.4:0, label: 26 <<<< tunnel head-end.
```

So the traffic to 192.168.200.200 should also be double tagged as shown below:

```
PE1# show ip cef 192.168.200.200
192.168.200.200/32
    nexthop 192.168.100.100 Tunnel10 label 26
```

However traffic is leaving the router only with the tunnel label:

```
PE1# trace 192.168.200.200
Type escape sequence to abort.
Tracing the route to 192.168.200.200
  0 192.168.12.2 [MPLS: Label 20 Exp 0] 4 msec 0 msec 0 msec
  1 192.168.23.3 [MPLS: Label 23 Exp 0] 4 msec 0 msec 0 msec
  2 192.168.34.4 4 msec 0 msec 0 msec
  3 192.168.48.8 4 msec * 4 msec
```

- CSCtg42904

Symptoms: Router crashes with the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address after applying the flow monitor to
virtual-template interface
```

Conditions The symptom is observed on a router configured with EasyVPN.

Workaround: There is no workaround.

- CSCtg51476

Symptoms: Cisco ISR G2 routers reload on their own with a bus error.

Conditions: This symptom is observed when BFD is configured.

Workaround: Remove BFD.

- CSCtg57831

Symptoms: In the event of a failover, there is a serial number mismatch on the active and standby.

Conditions: The symptom is observed in an High Availability CA servers environment, using Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtg58786

Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

Workaround: There is no workaround.

- CSCtg63096

Symptoms: The **deny ip any any fragments** command shows a high number of hits for traffic that may not be truly fragmented.

Conditions: This symptom occurs when “deny ip any any fragments” may be configured at the top of the ACL.

Workaround: There is no workaround.

- CSCtg71332

Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

Workaround:

1. Use SP services feature set.
2. Upgrade router to Cisco IOS Release 12.4(24)T.
3. Install one or more PVDM sLOTS.

- CSCtg91201

Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

Workaround: There is no workaround.

- CSCtg91336

Symptoms: A Cisco router may crash during show command **show ip ospf rib** execution.

Conditions: This symptom is observed in Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

- A user enters the **show ip ospf rib** command and stops in the middle.
- The OSPF local rib is significantly changed; for example, routes are removed.
- A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

Workaround: Do not enter the **show ip ospf rib** command. If it is necessary to use the command, enter **terminal length 0** and print the entire output.

- CSCtg92783

Symptoms: Uplink performance degrades by about 70% with HWIC-3G-CDMA when bound to external dialer interface when compared to using cellular interface legacy DDR.

Conditions: This symptom is seen on live network when performance is measured using latency sensitive Internet speed test application.

Workaround: Use cellular interface without binding to external dialer.

- CSCtg94250

Symptoms: Removing **address-family ipv4 vrf vrf** (in router BGP) followed by **no ip vrf vrf** (where “vrf” is the same) could result in a crash.

Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

1. **no address-family ipv4 vrf vrf**
2. **no ip vrf vrf**
3. **ip vrf vrf**

The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).
2. Give sufficient time for (1) to complete before applying (2).

- CSCtg95940

Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

Workaround: There is no workaround.

Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCth06812

Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1 (XNE1) and the following configuration:

```
R1(config)# parser view SUPPORT
R1(config-view)# secret cisco
R1(config-view)# commands exec include ping
R1(config-view)# commands exec include configure terminal
R1(config-view)# commands exec include show ip ospf neighbor <--Where we see the hang.
```

Workaround: Do not configure “commands exec include show ip ospf neighbor” command in parser view configuration.

- CSCth15268

Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.

Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit on.

Workaround: Set “llc2 local-window” to 1.

- CSCth16011

Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

Conditions: Introduce loss to network.

Workaround: There is no workaround.

- CSCth29426

Symptoms: When you issue a **reload** command with a getmany looping on ciscoFlashMIB, the router hangs.

Conditions: The symptom is observed when a getmany is running with only one router. The chances of hitting the issue seem to be increased if a **write memory** has been done before reload or even if the configuration is dirty and you respond “no” to the save configuration prompt.

Workaround: Avoid reloading while doing an SNMP walk on ciscoFlashMIB.

- CSCth31395

Symptoms: A Frame Relay PVC stays in the INACTIVE state.

Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

Workaround: There is no workaround.

- CSCth33457

Symptoms: A Cisco IOS router configured with IPSec (IP Security) may reload when receiving encrypted packets.

Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

- ip accounting precedence input
- ip accounting mac-address input
- WCCP
- Flexible NetFlow
- BGP accounting
- uRPF
- mpls accounting experimental input

Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth33500

Symptoms: NAS port is reported as zero on LNS.

Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

Workaround: There is no workaround.

- CSCth36114

Symptoms: A crash is seen after executing the **write memory** command via SDM.

Conditions: The symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

Workaround: Use Cisco IOS 12.4 versions.

- CSCth36740

Symptoms: A router may experience CRC and Runt errors.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2 and when the on-board GigabitEthernet interface is hard-coded to 10mb/full duplex. It is seen with the following routers: Cisco 1900 series, Cisco 2900 series, and Cisco 3900 series.

Workaround: There is no workaround.

- CSCth37092

Symptoms: A crash is observed in the PKI-HA feature when the standby tries to sync up with the active router.

Conditions: When the PKI server is created on the active router with a “database archive password” configuration, the PKI server is cloned on the standby. Soon after, the active router crashes.

Workaround: There is no workaround.

- CSCth38699

Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-Group mappings.

- CSCth45413

Symptoms: The environmental alarm has additional hard disk drive information in the Syslog message.

Conditions: The symptom is observed when there is one of the following service modules in the system:

- SM-SRE-900-K9
- SM-SRE-700-K9
- NME-APPRE-522-K9
- NME-APPRE-502-K9
- NME-APPRE-302-K9
- NME-WAE-502-K9
- NME-NAM-120S
- NME-NAM-80S
- NME-NAC-K9
- NME-CUE
- NME-UMG-EC
- NME-UMG

Workaround: There is no workaround.

- CSCth49421

Symptoms: Transparent bridging stops working.

Conditions: The symptom is observed when the interface goes to standby from active. The output of **show controllers gigabitethernet slot/port** shows these fields (at the end of output):

When working:

```
Software filtered frames: 0
  Unicast overflow mode: 1 <--
  Multicast overflow mode: 1
  Promiscuous mode: 1
  Total Number of CAM entries: 8
  Port Stopped: N
```

When not working:

```
Software filtered frames: 0
  Unicast overflow mode: 0 <--
  Multicast overflow mode: 1
  Promiscuous mode: 1
  Total Number of CAM entries: 4
```

Port Stopped: N

Workaround: Remove bridging and reconfigure it on the interface.

- CSCth58283

Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

Conditions: NAT is enabled.

Workaround: There is no workaround.

- CSCth62854

Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

Workaround: There is no workaround.

- CSCth64271

Symptoms: Routers in redundant configuration end up in Manual Swact = disabled.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCth65072

Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth69361

Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.

Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.

Workaround: There is no workaround.

- CSCth77531

Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU in the BGP-related processes for several hours (greater than 2.5).

Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process takes the most CPU; also, the number of routemap-cache entries should be very high.

```
Router# show ip bgp sum
```

```
BGP router identifier 1.1.1.1, local AS number 4739
```

BGP table version is 1228001, main routing table version 1228001 604000 network entries using 106304000 bytes of memory
 604000 path entries using 31408000 bytes of memory
 762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
 381 BGP AS-PATH entries using 9144 bytes of memory
 382 BGP community entries using 9168 bytes of memory
 142685 BGP route-map cache entries using 4565920 bytes of memory

Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results and the issue will not be observed.

- CSCth83508

Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

Conditions: The problem is seen when using WSMA to run the **session install** command.

Workaround: Perform the install manually from a VTY session.

- CSCth84995

Symptoms: Router may reload when performing an ISSU upgrade or downgrade.

Conditions: This symptom occurs when performing an ISSU upgrade or downgrade.

Workaround: There is no workaround.

- CSCth87587

Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

Workaround: There is no workaround.

Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth87638

Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

Conditions: The symptom is observed on WIC-based platforms. It was seen originally on an Cisco IAD243x using a HWIC-CABLE-D-2.

Workaround: Manually change the MAC address problem card.

Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- CSCth97996

Symptoms: A Cisco 39xx router may crash.

Conditions: The symptom is observed during regular operations and with an extensive QoS configuration. The issue is seen when running Cisco IOS Release 15.0(1)M3.

Workaround: There is no workaround.

- CSCth99237

Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

Conditions: The symptom is observed under the following conditions:

1. If the client starts to send LCP echo requests during the PPP Authentication phase.
2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

Workaround: There is no workaround.

- CSCti08336

Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are “IN” policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go “Out” of policy.

Workaround: There is no workaround.

- CSCti10016

Symptoms: After the **format** command is run on a 32GB or larger disk, the **show** command displays that only 4GB is free on the device.

Conditions: The symptom is observed when formatting disk that is larger than 32GB in capacity.

Workaround: Use a smaller size disk that has no more capacity than 32GB.

- CSCti10518

Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

Workaround: There is no workaround.

- CSCti13286

Symptoms: Putting this configuration on a router:

```
router rip
  version 2
  no validate-update-source
  network 10.0.0.0
  no auto-summary
  !
  address-family ipv4 vrf test
    no validate-update-source
    network 172.16.0.0
    no auto-summary
  version 2
  exit-address-family
```

and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti17190

Symptoms: A router crashes when trying to do sre install.

Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

Workaround: There is no workaround.

- CSCti19627

Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

Workaround: Remove “call-park system application”.

- CSCti22091

Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

Conditions: The symptom is observed when PfR is configured with the following conditions:

1. list > application > filter > prefix-list
2. Learn > traffic-class: keys
3. Learn > traffic-class: filter > ACL

Workaround: There is no workaround.

- CSCti25280

Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

```
**ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
```

Conditions: The symptom is observed when there is also a VWIC installed in the chassis (for example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

Workaround: Remove the VWIC.

- CSCti26202

Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

Conditions: The symptom is observed on a Cisco 3900 series router.

Workaround: There is no workaround.

- CSCti47649

Symptoms: A router may crash with the message:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04
```

Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

Workaround: There is no workaround.

- CSCti54173

Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

Conditions: The symptom is observed on a Cisco 7200 series router.

Workaround: There is no workaround.

- CSCti55261

Symptoms: On a phone button that has an overlay with call waiting DN's configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

Conditions: The symptom is observed on a phone button that has an overlay with call waiting DN's and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

Workaround: There is no workaround.

- CSCti62226

Symptoms: Voice port(s) that are created with PRI/ds0 configurations are active even after shutting down those ports. Because of this, unconfiguring PRI/ds0 configurations throws an error.

Conditions: The symptoms are observed with Cisco IOS Release 15.0(1)M3 when shutting down the voice-port to unconfigure the controllers.

Workaround: Do **no shut** first then **shut**.

Further Problem Description: If you are running a script for regression which cannot be changed there is no workaround. If it is a user interactive case, the above workaround may help.

- CSCti72836

Symptoms: The router crashes when removing an ACL.

Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hashtable.

Workaround: There is no workaround.

- CSCti75410

Symptoms: A Cisco 887 voice gateway is unable to detect any interface.

Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCti86169

Symptoms: A device that is acting as a DHCP relay or server crashes.

Conditions: This symptom is observed when the **no service dhcp** command is configured.

Workaround: There is no workaround.

- CSCti93398

Symptoms: A Cisco 1861 router reloads.

Conditions: The reload occurs upon booting.

Workaround: There is no workaround.

- CSCtj00039

Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj05198

Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

Conditions: This symptom is observed when there are two EIGRP router processes.

Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07885

Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

Workaround:

1. Configure CME-as-SRST with “srst mode auto-provision all”.
2. Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:
 - a) Stop the MIB on the NMS device that is doing the polling.
 - b) Turn off SNMP polling on the device.
 - c) Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj32574

Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

```
router eigrp 1
 redistribute connected
 no redistribute connected
```

The **no redistribute connected** command is not being backed up to the standby.

Conditions: This symptom is observed with any redistribute-related commands.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(1)T1

Cisco IOS Release 15.1(1)T1 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T1 but may be open in previous Cisco IOS releases.

- CSCsl64247

Symptoms: Router crashes 20-30 minutes after configuring “mode route control”.

Conditions: The symptom is observed when the router is configured as OER master.

Workaround: There is no workaround.

- CSCso20810

Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. Occurs when multicast subsequently flows out a crypto-enabled interface.

Conditions: This bug will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCsu31853

Symptoms: TCP sessions in TIMEWAIT state cause buffer usage until they move to CLOSED state.

Conditions: This symptom is observed with almost all TCP applications. It is mainly seen on low end switches.

Workaround: There is no workaround.

- CSCsx56362

Symptoms: BGP selects paths which are not the oldest paths for multipath. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps.

Conditions: The symptom is observed when:

1. BGP is configured.
2. More than one equally-good route is available.
3. BGP is configured to use less than the maximum available number of multipaths.

Workaround: There is no workaround.

Further Problem Description: The selection of non-oldest paths as multipaths is only problematic in releases which include CSCsk55120, because in such releases it causes changes with respect to whether paths are considered multipaths.

- CSCsz70049

Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the telco side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.

Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.

Workaround: Issue the **clear interface bri** command to restore this state.

- CSCta58068

Symptoms: During BGP convergence, a CPU spike may be seen on the local PE in an MVPN configuration.

Conditions: The symptom may be observed with the following conditions:

- Remote PE neighbor switchover.
- On local PE, do a **clear ip bgp nbr**.
- On bringup of local PE.
- Large configurations, such as one with 300 MDT default tunnels.

The following is an example of an MVPN configuration where this problem can be seen:

1. OSPF routing protocol is enabled on all the networks in the topology.

2. Each PE router has 100 MVRFs defined (between vpn_0 to vpn_99).
3. MDT default is configured on all the mVRFs on the PE routers.
4. PE routers have an iBGP session, ONLY with the RR (route-reflector).
5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes.
6. OSPF session also exists between Routem and PE1, with Routem sending 100 OSPF routes.

In effect, the following states are present in the network:

On PE and RR routers:

1. IGP states = 100 OSPF routes.
2. BGP states = 200,010 VPNv4 routes.

On PE routers ONLY:

1. VRF sessions = 100 VRFs (vpn0 to vpn_99).
2. MDT sessions = 100 SSM sessions.

Workaround: There is no workaround.

- CSCtb32892

Symptoms: Tracebacks such as:

```
%MFIB-3-DECAP_OCE_CREATION_FAILED: Decap OCE creation failed
```

may be seen on a router console when loading an image or during an RP SSO.

Conditions: The symptom is observed upon reloading a Provider Edge (PE) router with an mVPN configuration or during a simple SSO. It is observed on the standby RP.

Workaround: There is no workaround.

- CSCtb92791

Symptoms: The command **ip ospf message-digest-key** in interface mode may have an invalid key.

Conditions: The symptom is observed when “parser config cache interface” is configured.

Workaround: Use the command **no parser config cache interface**.

- CSCtc59535

Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

Workaround: Unplug and plug back the cable.

- CSCtc68910

Symptoms: Unnecessary retransmission and spurious TCP is reset.

Conditions: The symptom is observed when using NAT and a large (already fragmented) “updatecapabilitiesversion2” traverses the router.

Workaround: There is no workaround.

Further Problem Description: This problem seems to be correlated to:

- IP phone presents an updatecapabilitiesversion2 large packet (i.e.: 2012 bytes) fragmented (i.e.: in 4 pieces).

- CSCtd27247

Symptoms: The router crashes when doing concurrent VRF add and deletion configurations.

Conditions: The symptom is observed when a multiple configuration terminal is doing concurrent VRF add and deletion configurations.

Workaround: Do not do concurrent VRF addition and deletion.

- CSCtd34887

Symptoms: Performing a shut and no-shut on a subinterface with igmp-join causes SSM VRF mroute to disappear.

Conditions: SSM VRF mroute present in the table:

```
ce#show ip mroute vrf management
(Src 1 IP, Grp IP), 00:10:48/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
(Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
```

configuration of the interface:

```
int FastEthernet4.3
 encapsulation dot1Q 33
 ip vrf forwarding management
 ip address <IP addr> 255.255.255.252
 ip pim sparse-mode
 ip igmp join-group <group addr> source 10.32.178.56
 ip igmp join-group <group addr> source 10.32.178.23
```

Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, the **no ip igmp-join** and **ip igmp join** commands are entered on the interface.

- CSCtd47338

Symptoms: The following error message is constantly displayed:

```
crypto_engine_ps_vec(): no subblock attached
```

Conditions: This issue is observed on a Cisco 7200 series router with VSA cards, that is running Cisco IOS Release 12.4(15)T (other releases may be affected as well) and with DLSw configuration.

Workaround: Configure the command **dls w udp-disable**.

- CSCtd90367

Symptoms: Router crashes every 2-3 days with URLF feature. The error message shows memory leak issues.

Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(24)T2, with URLF features on the device.

Workaround: There is no workaround.

- CSCtd92028

Symptoms: The router reloads.

Conditions: The symptom is observed when a VRF is unconfigured while there are one or more WCCP service groups configured with that VRF.

Workaround: Unconfigure the relevant WCCP service groups prior to unconfiguring the VRF.

- CSCtd94789

Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCtd97164

Symptoms: LLQ packet drops on an ATM interface.

Conditions: The symptom is observed when having QoS under an ATM interface. Packet drops are seen under a class with “priority”, even though they have not reached the value configured. It does not matter if it is percent or absolute value.

Workaround: There is no workaround.

- CSCte02973

Symptoms: Routing protocols like EIGRP may be dropped in the global table.

Conditions: The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

Workaround: Enable “ip multicast routing” and create a loopback interface with “ip pim sparse-mode” enabled.

Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.

- CSCte10790

Symptoms: A Cisco Catalyst 6500 series switch may unexpectedly reload due to bus error on the switching processor when making access list entry config changes or when removing an entire access-list.

Conditions: This bug fixes two related crashes. One in which the crash occurs when making ace configuration changes and another when removing an entire ACL.

Details on the conditions to trigger the crash when making the ace configuration changes:

This can be reproduced in all the branches and the basic criteria reproducing this is we should have ACE is greater than 13, and we should have the extended ACE that has destination IPADDR.

The issue is seen when we have more than three ACE which have the same source and destination address and mask and we delete the ACE in sequence like:

```
no 110
no 120
no 130
```

Then try to add ACE which has the same source address and mask but no destination. The infinite loop will result in crash.

```
120 ACE
130 ACE
```

CRASH will happen

Follow the same order:

```
ip access-list extended vlan959-out
```

```

permit ip 128.227.128.52 0.0.0.3 any
remark - Standard out ACL -
permit tcp any any established
deny tcp any any eq 707
deny tcp any eq 707 any
deny tcp any any eq 4444
deny tcp any eq 4444 any
deny udp any any eq 31337
deny tcp any any eq 12345
deny tcp any any eq 12346
deny tcp any any eq 20034
deny tcp any any eq 7597
deny ip host 0.0.0.0 any
remark - allow cns & UFAD networks
permit ip 128.227.212.0 0.0.0.255 any
permit ip 10.227.212.0 0.0.0.255 any
permit ip 10.228.212.0 0.0.0.255 any
permit ip 10.249.10.0 0.0.0.255 any
permit ip 128.227.74.0 0.0.0.255 any
permit ip 128.227.156.0 0.0.0.255 any
permit ip 128.227.0.240 0.0.0.15 any
permit ip 10.5.187.240 0.0.0.15 any
permit ip 10.241.28.240 0.0.0.15 any
permit ip 128.227.128.112 0.0.0.3 any
permit udp 128.227.128.0 0.0.0.255 eq ntp 10.241.33.0 0.0.0.255
permit udp 128.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
permit tcp 128.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
permit tcp 128.227.156.0 0.0.0.255 host 10.241.33.11 eq www
permit tcp 128.227.128.0 0.0.0.255 host 10.241.33.29 eq cmd

```

Then follow the order:

```

no 110
no 120
no 130
120 permit udp 128.227.128.0 0.0.0.255 eq domain any
130 permit tcp 128.227.128.0 0.0.0.255 eq domain any

```

Workaround: The ACE configuration change crash can be worked around by deleting the entire ACL and then add the resequenced ACE.

The crash when removing the access-list itself has no workaround.

- CSCte14955

Symptoms: A Cisco ASR 1000 Series Aggregation Services router may experience an unexpected reload.

Conditions: The symptom may occur when multiple tunnel interfaces are configured with **mpls bgp forwarding**, if the tunnel interfaces are flapping.

Workaround: Configure the eBGP sessions on interfaces other than tunnel interfaces.

- CSCte17284

Symptoms: A router may unexpectedly reload due to software forced crash because of chunk memory corruption.

Conditions: The crash appears to happen when using the clientless web proxy method. The crash is triggered by accessing a webpage through the SSL VPN with a URL longer than 1009 characters long.

Workaround: If possible, redesign the website to use URLs of 1009 characters or shorter.

- CSCte38855

Symptoms: Chunk leak is seen after exec-timeout expires.

Conditions: The symptom is observed after the **interface range** command is configured and when the console timeout expires.

Workaround: There is no workaround.

- CSCte39643

Symptoms: If PfR receives an EIGRP route change, the router may unexpectedly reload.

Conditions: The symptom is observed with PfR and EIGRP configurations. It is observed some time after PfR receives an EIGRP route change, but before the previous EIGRP route is removed in the routing table, when PfR tries to recycle a previous EIGRP route.

Workaround: There is no workaround.

- CSCte41410

Symptoms: TCP connections may get stuck when using SSLVPN with **webvpn cef** configured. These connections will be stuck in TIMEWAIT state and will not timeout after the usual minute or so and will stay around forever.

Conditions: This symptom occurs when using SSLVPN with **webvpn cef** configured.

Workaround: Issue the **no webvpn cef** command.

- CSCte48009

Symptoms: The NAS-Port and NAS-Port-ID AAA Attributes are not sent in radius messages.

Conditions: The symptom is observed if the VCI value configured on the interface is larger than 32767.

Workaround: Use VCI values less than 32767.

- CSCte49283

Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

Workaround: There is no workaround.

- CSCte54807

Symptoms: Configuring PVC with Cisco IOS Release 15.0(1)M1 brings up a virtual-access interface, right after sending the ConfReq, even if there is no reply.

Conditions: The symptom is observed when using a PPPoA setup on Cisco IOS Release 15.0(1)M1. It is seen only if some unused ATM PVCs are present at one end with the PPP configurations applied on them.

Workaround: Use Cisco IOS Release 12.4(24)T2.

- CSCte62453

Symptoms: Performing a shut and no-shut on a subinterface with igmp-join causes SSM VRF mroute to disappear.

Conditions: This symptom is observed when SSM VRF mroute is present in the table:

```
ce#show ip mroute vrf management (Src 1 IP, Grp IP), 00:10:48/stopped, flags: sPLTXI
Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
Outgoing interface list: Null
(Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
Outgoing interface list: Null
```

In addition, the interface is configured as follows:

```
int FastEthernet4.3
encapsulation dot1Q 33
ip vrf forwarding management
ip address <IP addr> 255.255.255.252
ip pim sparse-mode
ip igmp join-group <group addr> source 10.32.178.56
ip igmp join-group <group addr> source 10.32.178.23
```

Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, the **no ip igmp-join** and **ip igmp join** commands are entered on the interface.

- CSCte63156

Symptoms: Router hangs and crashes when a DHCP pool configured with “origin aaa subnet” is removed.

Conditions: The symptom is observed when pool is configured with “origin aaa subnet ...” and without unconfiguring this command, the pool is deleted with the **no ip dhcp pool** command. Also missing is “aaa accounting” with “default method-list” from global configuration.

Workaround: Globally configure “aaa accounting” with “default method-list” (“aaa accounting network default”).

- CSCte76513

Symptoms: If ZBF and WAAS are configured on a router, you may see drop logs similar to the following:

```
%FW-6-DROP_PKT: Dropping tcp session x.x.x.x y.y.y.y due to No zone-pair between zones
with ip ident 0

%FW-6-DROP_PKT: Dropping http session x.x.x.x y.y.y.y on zone-pair admin-to-wan class
admin due to Invalid Flags with ip ident 0
```

Conditions: The symptom is observed if ZBF and WAAS are configured on a router.

Workaround: There is no workaround.

- CSCte78165

Symptoms: Device may reload when the **show ip protocol** command is issued.

Conditions: The symptom is observed when routing protocol is configured and the ISIS routes are being redistributed.

Workaround: Do not use the **show ip protocol** command.

- CSCte82917

Symptoms: On a Cisco 7600 series RSP720, the **show proc cpu sort** command displays a CPU utilization of 0, but the per-process CPU utilization is 100% for some processes; no packet loss occurs, however.

Conditions: This symptom is observed under the following conditions:

- The router is decently loaded.
- HSRP is enabled in an HA environment.
- A large number of HSRP sessions are established.

Workaround: Reduce the number of HSRP sessions to only a few. The router does not see any performance or functional impact. This is an issue only with internal CPU accounting.

- CSCte83779

Symptoms: A Cisco ASR 1000 Series Aggregation Services router may crash.

Conditions: The symptom is observed when DMVPN is configured with GETVPN. It is only seen when running a specific script for ASRs.

Workaround: There is no workaround.

- CSCte89436

Symptoms: Router crashes.

Conditions: The symptom is observed when encapsulation is changed from from “frame-relay” to “hdlc”.

Workaround: There is no workaround.

- CSCte96453

Symptoms: Switch intermittently crashes when configuring energywise features.

Conditions: The symptom is observed when the port is configured with “energywise level 10” to bring up a previously down port.

Workaround: There is no workaround.

- CSCte98082

Symptoms: PPPoE session is not coming up on some clients due to a malformed PADO. PPPoE relay sessions are failing to come up on an LAC.

Conditions: The symptom is observed with a few clients which are unable to process malformed PADO and also when “pppoe relay service” is configured on the LAC.

Workaround: There is no workaround.

- CSCtf00427

Symptoms: A router may experience a severe memory leak issue when the following command is configured:

privilege exec level *level* show ip ospf neighbor

Conditions: The symptom is observed when running Cisco IOS Release 12.2(33)XNE or 12.2(33)XNE1. The issue is not platform dependent.

Workaround: Reload the router.

- CSCtf04954

Symptoms: When the **cns config notify** command exists, some CLIs might misbehave or cause unexpected crashes during the configuration change.

Conditions: The symptom is observed with the **cns config notify** command.

Workaround: Remove all **cns config notify** CLIs from the configuration.

- CSCtf06436

Symptoms: Continuous high CPU usage.

Conditions: The symptom occurs after the formation of a recursion loop in the FIB, when the prefixes in the loop are labeled.

Workaround: There is no workaround.

- CSCtf08864

Symptoms: Incoming ISDN T1/E1 PRI voice calls may disconnect or fail to complete properly.

When an incoming call is made, the following symptoms may be noticed in the output of **debug isdn q921** and/or **debug isdn q931**:

1. Q.921 debugs may report "***ERROR**": L2_AdvanceVA: TX_ack_queue empty", after which the B-channel used for the call attempt locks up. The ISDN provider needs to reset the B-channel in order to return it to service.
2. Q.931 debugs may show that a voice call disconnected prematurely.
3. Q.921 debugs may intermittently duplicate messages such as Receiver Ready (RR) Polling exchanges, Info frames, or SABME frames.

Conditions: The symptom is observed on a Cisco ISR G2 2900/3900 Voice Gateway which has been installed with a VWIC2 T1/E1 MultiFlex Trunk card, configured for ISDN PRI voice services, and running a Cisco IOS 15.0 or 15.1T release. The following conditions are observed:

1. The VWIC2 generation of T1/E1 MultiFlex Trunk cards must be used.
2. This is a problem affecting PRI voice installs. Data PRI installs are not affected.
3. This is an ISR G2 2900/3900 platform-specific issue.

Not all PRI voice installs will be affected by this problem. It depends on how HDLC is configured on the PRI lines by the provider. To be specific, if the provider sends marks (all-ones) instead of HDLC flags during idle times, the call completion problem may manifest itself. Most provider installations are not configured this way and the provider may be able to switch the method of indicating an idle.

Workaround 1: Ask the service provider to send flags between frames instead of idle marks. Idle marks (1111111) may be sent to fill the gap between useful frames. Alternatively, a series of flags (01111110) may be transmitted to fill gaps between frames instead of transmitting idle marks. Continuous transmission of signals is required to keep both the transmitting and receiving nodes synchronized.

Workaround 2: If Workaround 1 is not possible, a Cisco IOS image with a candidate fix is available. The candidate fix has a high confidence level of resolving the PRI voice call issues described above, and has proven to be successful in several field deployments complaining of similar call problems. Please contact the Cisco Technical Assistance Center (TAC) for details on obtaining the candidate fix.

- CSCtf18077

Symptoms: A CME router may unexpectedly reload due to a bus error when a Cisco Unified Contact Center Express (UCCX) unregisters from the CME.

Conditions: The symptom is observed when the Cisco UCCX unregisters from the CME.

Workaround: There is no workaround.

- CSCtf18524

Symptoms: Throughput performance for HTTP traffic is impacted.

Conditions: The symptom is observed when the SSLVPN feature is configured on the router and crypto engine is configured to accelerate the SSLVPN feature.

Workaround: There is no workaround.
- CSCtf19461

Symptoms: IP address is not leased out to the client from server.

Conditions: The symptom is observed when configuring the VPN sub-option at the interface level on the relay.

Workaround: There is no workaround.
- CSCtf25293

Symptoms: SSH connection to a SSH server aborts abruptly after making the connection, while using public key-based authentication.

Conditions: Authentication method used must be public key.

Workaround: Use kbd-interactive or password-based authentication.
- CSCtf27303

Symptoms: On a Cisco router, a BGP session for a 6PE (peer-enabled in AF IPv6 and end-label configured) with a third-party router, which does not advertise capability IPv6 unicast (not AFI 2 SAFI 1, only AFI 2 SAFI 4) may be torn down right after it establishes, as the Cisco router sends out an update in the non-negotiated AF IPv6 unicast (AFI/SAFI 2/1).

Conditions: The symptom is observed under the following conditions:

 - Cisco side: session enabled for IPv6 + send-label. Cisco router is running Cisco IOS Release 12.2(33)XNE1 and Release 12.2(33)SRE.
 - Third-party: only capability IPv6 labeled unicast advertised.

Workaround: There is no workaround.
- CSCtf27324

Symptoms: A ping from a CPE (which is doing PPP to the IP address of the LNS router that terminates that PPP call) fails. PPP has been opened and IPCP has negotiated an IP address. Ping from the LNS back to the CPE works fine. Between the LAC and the LNS there is a PPP multilink bundle.

Conditions: The symptom is observed only when there is a plain PPP call from a client (ISDN modem or dial up modem which is doing PPP). In addition, the physical connectivity between the LAC and the LNS is PPP multilink.

Workaround: Disable CEF on the physical interface between the LAC and the LNS. If the CPE is doing PPP multilink, the ping works fine.

Further Problem Description: The issue seems to be specific with the forwarding of the packets through the PPP multilink bundle that exists between the LAC and the LNS.
- CSCtf29685

Symptoms: PPPoE server router crashes upon sending an accounting stop request.

Conditions: The symptom is observed with a PPPoE setup for both PTA and forwarded case. This is seen only if template authorization is enabled (i.e.: “aaa authorization template” is configured) and some template attributes are configured in the user-profile on the radius server.

Workaround: There is no workaround.

- CSCtf31067

Symptoms: There is no implementation for retransmitting MS-CHAP v2 challenge for PPP negotiation.

Conditions: The symptom is observed with a MS-CHAP v2 challenge.

Workaround: There is no workaround.

- CSCtf36117

Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

Workaround: There is no workaround.

- CSCtf39455

Symptoms: Router can hang when xconnect configuration is modified on a VLAN subinterface while data packets are being switched. The following error traceback is printed:

```
%SYS-2-NOTQ: unqueue didn't find 0 in queue
```

Conditions: The symptom is observed when the VLAN subinterface is still seeing data traffic and the main interface is not shut down, and when the xconnect configuration on the VLAN subinterface is being modified.

Workaround: Shut down the main ethernet interface when doing xconnect configuration changes on the subinterface.

- CSCtf40425

Symptoms: When executing the **service-module interface install** command on an SRE module on a Cisco Integrated Services Router (ISR) G2, the router may unexpectedly reload due to a bus error.

Conditions: The symptom is observed only when executing the install on an SRE module.

Workaround: There is no workaround.

- CSCtf40731

Symptoms: A routing loop is unexpectedly formed when PIRO and an OER-generated static route works together.

Conditions: The symptom is observed under the following conditions:

1. PIRO generates a more specific prefix for the static route it has created.
2. OER-generated static route is redistributed into other IGP protocol in order to get traffic.

Workaround: There is no workaround.

- CSCtf47335

Symptoms: Wrong typedef version is returned.

Conditions: The symptom is observed on getTypedefs CT, the typedefVersion returned is "2008-08-01". This is the wrong version with some undefined entries. Due to this, the signature parsing is failing in CCP.

Workaround: There is no workaround.

- CSCtf47396
Symptoms: A Cisco router may crash when a service-policy configured with bandwidth is removed from an interface.
Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 15.1(1)T.
Workaround: There is no workaround.
- CSCtf50075
Symptoms: A traffic blackhole can occur.
Conditions: The symptom is observed following shut/unshut/shut of the redundant forwarding interface.
Workaround: There is no workaround.
- CSCtf51690
Symptoms: Router crashes when a packet with out-of-bound featureIndex values is sent to the CME.
Conditions: The symptom is observed when malformed packets are sent to the CME with out-of-bound featureIndex values in fStationFeatureStatReqMessage.
Workaround: There is no workaround.
- CSCtf52106
Symptoms: There is a failure of EEM TCL scripts when using the “exit_comb” keyword for the Interface Event Detector.
Conditions: The symptom is observed when using the “exit_comb” keyword in an EEM TCL script.
Workaround: There is no workaround.
- CSCtf57641
Symptoms: A router crashes after performing a DNS lookup.
Conditions: The symptom is observed when a command is used which sends out a DNS query such as **ping www.cisco.com** and the DNS server response contains a specially crafted packet.
Workaround: Configure “no ip domain-lookup”.
- CSCtf62621
Symptoms: Unable to push the firewall down to the VDSL chipset on a Cisco 887V modem.
Conditions: The symptom is observed on a Cisco 887V router with no startup configuration in NVRAM.
Workaround: Perform a **write memory** and reload the router.
- CSCtf66271
Symptoms: A Cisco ASR 1000 Series Aggregation Services router that was running the asr1000rp1-adventerprisek9.02.04.02.122-33.XND2.bin image and then upgrades to the asr1000rp1-adventerprisek9.02.06.00.122-33.XNF.bin image displays the complete certificate chain as follows:

```
crypto pki certificate chain JUTnetRoot-Pilot certificate ca
3C5A00179190F2DF23325330195B9B67 308203AE 30820296 A0030201 0202103C 5A001791 90F2DF23
32533019 5B9B6730 0D06092A 864886F7 0D010105 05003071 310B3009 06035504 06130255
53311930 17060355 040A1410 41542654 20436F72 706F7261 74696F6E 311F301D 06035504
0B131646 6F722054 65737420 50757270 6F736573 204F6E6C <truncated>
```


whereas before the upgrade it displayed:

```
crypto pki certificate chain JUTnetRoot-Pilot certificate ca
3C5A00179190F2DF23325330195B9B67 nvram:ATTCorporati#9B67CA.cer
```

Conditions: The symptom is observed with a Cisco ASR 1006 router that is running the asr1000rp1-adventerprisek9.02.06.00.122-33.XNF.bin image.

Workaround: There is no workaround.

- CSCtf67170

Symptoms: There is a crash due to the following error:

```
%ALIGN-1-FATAL: Illegal access
```

Conditions: The symptom is observed when “call monitor” is configured.

Workaround: Remove call monitor, if interfacing with UCCX is not needed.

- CSCtf70959

Symptoms: EzVPN client is trying to negotiate the connection with a NULL address when the outside interface is a profile-based dialer interface.

Conditions: This situation is a corner condition. The IP address on the dialer interface will be installed as soon as the dialer negotiation completes and the dialer interface comes up. But in this case, even though the IP address is not installed the dialer interface, the API is returning TRUE and proceeds further with the EzVPN connection.

Workaround: Use a non profile-based dialer interface.

- CSCtf71010

Symptoms: Traffic does not flow through the hub.

Conditions: The symptom is observed when a Cisco 3900 series router is configured for VRF-aware tunnel protection for IKEv2 sessions.

Workaround: There is no workaround.

- CSCtf71990

Symptoms: An alert message is not sent if “source-ip-address” is configured in the call-home configuration. The following message is shown:

```
%CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP servers (ERR
7, error in connecting to SMTP server)
```

Conditions: The symptom is observed when “source-ip-address” is configured.

Workaround: Remove “source-ip-address”.

- CSCtf75053

Symptoms: DHCP Relay will send a malformed DHCP-NAK packet. The malformed packet will be missing the END option (255) and the packet’s length will be truncated to 300. In effect, all the options after 300 bytes, if any, will be missing.

Conditions: When a Cisco 10000 series router is configured as a relay and a DHCP request is sent from the CPE, the router will send a DHCP-NAK when client moves into a new subnet.

Workaround: There is no workaround.

- CSCtf78196

Symptoms: Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

Conditions: The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface. (It is seen on many images)

Workaround: Statically configure “ipv6 mtu <mtu>” on tunnel interfaces.

- CSCtf80105

Symptoms: When basic SIP-SIP calls are placed using automation scripts, calls start failing due to UDP socket connection error

Conditions: The symptom is observed when the router is configured with a dial peer and with SNMP. A dial peer is most likely required to reproduce the issue, but it is possible that a different UDP protocol other than SNMP could also cause the symptom. Once a call failure occurs, all the calls placed later will fail with a UDP socket connection error.

Workaround: Use the following steps:

1. Under sip-ua, configure “connection-reuse” (which is a hidden command).
2. Configure the use of TCP.

- CSCtf81271

Symptoms: When “station-id name” or “station-id number” is configured on a voice port, “caller-id enable” will also be configured on that voice port.

Conditions: The symptom is observed after upgrade to Cisco IOS Release 12.4(22)T or Release 12.4(24)T where the **caller-id enable** command gets auto-configured on the voice-port.

Workaround: Manually remove the **caller-id enable** command after a router reboot.

- CSCtf82883

Symptoms: When clearing a VRF route, there is a traffic drop on other VRF routes.

Conditions: The symptom is observed with an L3 VPN configuration.

Workaround: There is no workaround.

Further Problem Description: Some LTE broker distribution is leaked to other VRFs.

- CSCtf83092

Symptoms: Standby resets continuously while ISSU upgrade from a non-componenterized IOS image to a componenterized IOS image.

Conditions: The issue is seen with an MPLS VC configuration.

Workaround: There is no workaround.

- CSCtf83101

Symptoms: Packets are not correctly classified by QoS class-map in CEF switching. Priority packets are dropped even if they are classified into LLQ. This is shown by the **show policy-map interface** command.

Conditions: The symptom is observed under the following conditions:

- A BRI interface.
- LLQ is configured on egress port by policy-map.
- The following devices/platforms are used: HWIC-4B-S/T or HWIC-1B-U, Cisco 181x, Cisco 180x, Cisco 800.

Workaround: Disable CEF.

Alternate Workaround: Use the other HWIC or WIC.

- CSCtf85219

Symptoms: The following symptoms are seen:

 - No dial tone when going off hook, so other phone numbers cannot be dialed.
 - The hung port can receive incoming calls, however the originating phone hears ring back. The terminating phones rings but when the call connects there is one-way audio.

Conditions: The symptom is observed with STCAPP-controlled FXS ports.

Workaround: Perform a shut/no shut on the voice port. If this does not work, perform a reload.
- CSCtf86556

Symptoms: The middle router crashes when it receives a PathTear message.

Conditions: The symptom is observed when the middle router (that does not have SREFRESH configured) receives a PathTear message, when the session debug is on.

Workaround: Disable the session debugs.

Alternate workaround: Configure refresh reduction on the UUT.
- CSCtf87039

Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

Workaround: There is no workaround.
- CSCtf96538

Symptoms: ATM interface does not pass/receive traffic. The configuration on the ATM interface shows “atm scrambling cell-payload” configured, but the **show controller ATM** output shows “DS3 Scrambling OFF”.

Conditions: The symptom is observed on a Cisco 3925 router, with an NM-1A-T3/E3 and running a Cisco IOS 15.0 release.

Workaround: Disable scrambling on the network.
- CSCtf91428

Symptoms: Router crashes in IP Input.

Conditions: NAT needs to be configured.

The customer who reported the crash was using bit torrent when it has crashed.

The public interface was an ATM [DSL].

Workaround: Disable

ip nat service for h232 - rass

Disable CEF globally.
- CSCtf97322

Symptoms: Shaping is not working correctly. An additional symptom on a Cisco 2900 series router is the possibility of alignment errors and, in rare situations, a software-forced crash.

Conditions: The symptom is observed on Cisco 2900 and 3900 series routers when using one of the following serial modules: HWIC-1T, HWIC-2T and HWIC-1DSU-T1.

Workaround: There is no workaround.

- CSCtg02719
Symptoms: Informers reload.
Conditions: The symptom is observed when enabling the **voice dsp crash-dump** or **debug vpm dsp** commands. These two commands may cause Informers to reload.
Workaround: Do not enable the **voice dsp crash-dump** or **debug vpm dsp** commands on Informers.
- CSCtg06863
Symptoms: The **show processes cpu sorted** command will incorrectly show processes with CPU utilization of 100%. Also, CPU utilization will vary randomly.
Conditions: The symptom is always observed when traffic is flowing through the router and may or may not be seen without traffic flowing.
Workaround: There is no workaround.
- CSCtg07557
Symptoms: A reload of a Cisco 1941W-A/K9 causes the embedded AP 801 to go to ROMMON. The AP BOOT parameter is no longer set and the startup configuration is also erased.
Conditions: The symptom is observed when a reload is issued on the router and you reload the AP at the same time when prompted.
Workaround: When reloading router using CLI, answer “no” when prompted to reload the embedded AP. The embedded AP can be reloaded with the **service-module wlan-ap 0 reload** command from router console or the **reload** command from embedded AP console accessed via **service-module wlan-ap 0 session**.
- CSCtg08496
Symptoms: After merge, keyserver deletes all GMs so the rekey fails to be sent (DB is empty) and all the GMs need to re-register.
Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T2.
Workaround: There is no workaround.
- CSCtg09379
Symptoms: After upgrading to an IOS build with EnergyWise specification: (rel2_5)1.0.32, the switch crashes several hours later.
Conditions: The symptom is observed when activity check is on and recurrence is changed from 0 to a higher value.
Workaround: There is no workaround.
- CSCtg11186
Symptoms: A router may face a watchdog crash or hang while removing a port-channel.
Conditions: The symptom is observed with a Cisco 3900/2951 router when removing a port-channel interface. It is seen when PPPoE is enabled on the GE interface.
Workaround: There is no workaround.
- CSCtg13758
Symptoms: Router can crash due to corrupted magic value in freed chunk.
Conditions: The symptom is observed on a Cisco 881 router that is running Cisco IOS Release 12.4(24)T1.
Workaround: There is no workaround.

- CSCtg17600

Symptoms: The configured “egress-method negotiated-return” does not work.

Conditions: The symptom is observed with VRF-aware WCCP and with Cisco IOS Release 15.1(1)T. The WCCP return traffic arrives on a sub-interface.

Workaround 1: Do not configure “egress-method negotiated-return”.

Workaround 2: If “egress-method negotiated-return” is configured ensure that the interface on which return traffic arrives is not configured with sub-interfaces.

Workaround 3: Change the Cisco IOS Release from 15.1(1)T to 15.0M.

- CSCtg20254

Symptoms: Router crashes.

Conditions: The symptom is observed when “debug glbp event” is turned on.

Workaround: There is no workaround.

- CSCtg23251

Symptoms: Analog phones lock up and there is no dial tone.

Conditions: The symptom is observed when the CME is in fallback as SRST and a directed call park is attempted on analog phones. The user cannot pick up a call from a park slot by direct dialing the slot. In the event that the user is able to retrieve the call, when the call is hung up the channel is not released. No dial tone is heard when the handset is picked up again.

Workaround: Reset the ports.

- CSCtg28806

Symptoms: Router crashes at PKI manual enroll.

Conditions: The symptom is observed on a Cisco 2921 router that is running Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

- CSCtg36728

Symptoms: Router crash or spurious memory access can be seen.

Conditions: The symptom is observed if non-default locale is enabled and a UCME receives a make call request from UCXSI with the “prompt” option.

Workaround: There is no workaround.

- CSCtg38344

Symptoms: Upon a reload, a router may lose most of its configuration after the pubkey-chain user/server sub-mode is gone. The following error is reported during the reboot:

```
Installed image archive Cisco 1841 (revision 5.0) with 237568K/24576K bytes of memory.
Processor board ID 6 FastEthernet interfaces 2 Virtual Private Network (VPN) Modules 2
802.11 Radios DRAM configuration is 64 bits wide with parity disabled. 191K bytes of
NVRAM. 62720K bytes of ATA CompactFlash (Read/Write)
bridge irb ^ % Invalid input detected at '^' marker.
interface FastEthernet0/0 ^ % Invalid input detected at '^' marker.
```

Conditions: The symptom is observed on a router that is running Cisco IOS Release 15.0(1)M2 with “ip ssh pubkey-chain” configured.

Workaround: Remove the SSH keys before upgrading to Cisco IOS Release 15.0(1)M2 or Release 15.1(1)T.

- CSCtg40901
Symptoms: Crash seen while authenticating with TACACS.
Conditions: The symptom is observed if the TACACS server does not respond.
Workaround: Use multiple connections.
Alternate Workaround: Configure a dummy TACACS server.
- CSCtg41232
Symptoms: Traffic, set to be exempted from inspection via an extended ACL, is still inspected even though the ACL registers counts for that traffic.
Conditions: The symptom is observed on any Cisco access router that is running Cisco IOS 15.x code.
Workaround: There is no workaround.
- CSCtg41733
Symptoms: Certain crafted packets may cause memory leak on a Cisco IOS router.
Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.
Workaround: Disable SIP if it is not needed.
- CSCtg45099
Symptoms: Router crashes.
Conditions: The symptom is observed when the **show cca** command is issued.
Workaround: There is no workaround.
- CSCtg54272
Symptoms: Router may crash when upgrading modem firmware.
Conditions: The symptom is observed with a Cisco 880 router that is running Cisco IOS interim Release 15.1(0.26)T.
Workaround: There is no workaround.
- CSCtg56013
Symptoms: Router crashes when initiating ping through the modem after router bootup.
Conditions: The symptom is observed when the modem fails to enumerate at bootup.
Workaround: There is no workaround.
- CSCtg57623
Symptoms: Music on hold does not work with iLBC codec when an IOS transcoder is used.
Conditions: The symptom is observed when the phone is configured to use iLBC codec and a transcoder is invoked to transcode MOH G.711 audio stream to iLBC codec. The phone rejects the RTP stream due to incorrect payload-type (it sends payload type 118 instead of the correct 116 for iLBC).
Workaround: There is no workaround if iLBC codec is needed, but using a different codec at the remote phone should work.
- CSCtg57657
Symptoms: A router is crashing at dhcp function.
Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

Workaround: There is no workaround.

- CSCtg63942

Symptoms: The output of **show proc cpu sorted** is not correct. The total CPU displayed is always 0, even though the interrupt level CPU displayed is a non zero value. Total CPU should be the sum of the interrupt and process level CPU. Consequently, the values displayed by **show proc cpu history** are also incorrect.

Conditions: The symptom is observed when using the **show process cpu sorted** command.

Workaround: There is no workaround.

- CSCtg65763

Symptoms: The command **clear crypto gdoi** on the keyserver does not clear the keyserver policies.

Conditions: The symptom is observed once the keyserver policies have been created.

Workaround: There is no workaround.

- CSCtg73691

Symptoms: You cannot configure “route-target import” or other BGP extended community values with values greater than 65535 to the right of the “:” even though you are using a value less than 65536 to the left of the “:”.

Conditions: This is seen when you issue a route-target import command with a value less than 65536 to the left of the “:” (and no “.” to the left of the “:”) and a value greater than 65535 to the right of the “:”.

Workaround: There is no workaround.

Further Problem Description: This problem was introduced by CSCtf13343.

The following formats are supposed to be accepted:

1. <IPv4 address>:<16-bit number>.
2. <2-byte ASN>:<32-bit number>.
3. <4-byte ASN in asplain format>:<16-bit number>.
4. <4-byte ASN in asdot format>:16-bit number.

- CSCtg79105

Symptoms: A UC560 unexpectedly reboots.

Conditions: The symptom is observed when the **show memory 0** command is executed.

Workaround: There is no workaround.

- CSCtg86714

Symptoms: The **show cellular 0** command might not show any output.

Conditions: The symptom is observed with the **show cellular 0** command.

Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the “MODEM UP” line, you get “LINK UP” and still retain the **show cellular stats**.

- CSCtg88766

Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

- Workaround: There is no workaround.
- CSCtg93243

Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used packets get forwarded after decryption as expected.)

Workaround: There is no workaround.
 - CSCtg99114

Symptoms: The following error message with traceback is observed:

```
%IPC-5-REGPORTFAIL: Registering Control Port
```

Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.

Workaround: Drop IPC traffic using control-plane policing:

```
class-map match-all ipc
match access-group name ipc
policy-map drop-ipc
class ipc
drop
ip access-list extended ipc
permit udp any any eq 1975
control-plane
service-policy input drop-ipc
```
 - CSCth02789

Symptoms: System can crash when attempting to schedule an IPv6 icmp-echo operation.

Conditions: The symptom is observed with IPv6 and icmp-echo.

Workaround: There is no workaround.
 - CSCth15518

Symptoms: Ping through ISDN BRI interface fails.

Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.

Workaround: There is no workaround.
 - CSCth35620

Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

Conditions: The symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

Workaround: There is no workaround.
 - CSCth39774

Symptoms: UUT hangs when an eTCDF file is loaded on the router in the latest t_base_1 code base.

Conditions: The symptom is observed when an eTCDF file is loaded on the router, the UUT seems to hang. However, the UUT is actually waiting for user input, and if you enter “#” on the CLI, it will print some error messages about invalid commands and return to CLI.

Workaround: Do not use the eTCDF file to configure the encrypted filter, rather directly enter the commands on the CLI of the router.

- CSCth47765

Symptoms: Once a router boots up, FXS/FXO voice-port in slot2 stays in “S_OPEN_PEND” state. The DSP from the MB that provides resources to the EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards in slot 2 goes into “FW_DNLD_FINISHED” state which causes the voice ports on EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards to go into “S_OPEN_PEND state”.

Conditions: The symptom is observed with Cisco IOS interim Release 15.1(1) T0.9 with 26.8.0 DSPware.

Workaround: There is no workaround.

- CSCth51125

Symptoms: PCEX-3G-HSPA-R6 is not recognized at bootup:

```
%CISCO800-2-MODEM_NOT_RECOGNIZED: Cellular0 modem not RECOGNIZED. Carrier id not
available or invalid! Replace it with Cisco supported modem and reload the router.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
```

Conditions: The symptom is observed on a Cisco 881G-K9 that is running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCth59217

Symptoms: Firewall sessions are not seen when ZBFW and and gatekeeper are configured on the UUT.

Conditions: The symptom is observed when ZBFW and gatekeeper are configured on the UUT.

Workaround: There is no workaround.

- CSCth79353

Symptoms: A Cisco 3900 series router may experience a software-forced reload when running Cisco IOS Release 15.0(1)M1.

Conditions: The symptom is observed when the router has a QoS policy attached to one of the LAN interfaces. The QoS policy needs to match different ACLs and have shaping configured.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(1)T

All the caveats listed in this section are open in Cisco IOS Release 15.1(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsl64247

Symptoms: Router crashes 20-30 minutes after configuring “mode route control”.

Conditions: The symptom is observed when the router is configured as OER master.

Workaround: There is no workaround.

- CSCsm82554

Symptoms: A router may unexpectedly reload if the device runs out of memory and a call is setup.

Conditions: The symptom is observed in rare circumstances when the device is already out of memory.

Workaround: There is no workaround.

- CSCsu24321

Symptoms: Router crashes due to a bus error in IOS firewall.

Conditions: This symptom occurs on a Cisco 3825 router running Cisco IOS Release 12.4(20)T.

Workaround: There is no workaround.

- CSCsu64365

Symptoms: The system may experience repeated crash due to I/O memory corruption showing error messages like:

```
%SYS-6-BLKINFO: Corrupted next pointer blk
```

Conditions: The corruption is caused by voice packets encapsulated by GRE/IPSEC (other encapsulations which add to the size of the packet). The router must have voice packets routed through GRE or IPSEC tunnel and if a simultaneous Fax tone is sent, the router will crash.

Workaround: Move the GRE tunnel from the CME where ever possible.

- CSCsu66197

Symptoms: Cyclic redundancy check (CRC) errors increment on Cisco 2800 router.

Conditions: Occurs during normal operation.

Workaround: There is no workaround.

- CSCsv81150

Symptoms: A Cisco AS5400-XM may encounter the following error messages:

```
%SYS-2-MALLOCFAIL: Memory allocation of 190 bytes
failed from 0x6237F000, alignment 0 Pool: Processor Free: 630453896 Cause:
Interrupt level allocation
Alternate Pool: None Free: 0 Cause: Interrupt level allocation
-Process= "<interrupt level>", ipl= 3,
```

```
%SYS-3-INTPRINT: Illegal printing attempt from interrupt level.
```

```
%SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level,
```

```
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level,
```

Conditions: The symptom is observed with a Cisco AS5400-XM that is running Cisco IOS Release 12.4(15)XY2.

Workaround: There is no workaround.

- CSCsv86234

Symptoms: The Cisco Gateway GPRS Support Node (GGSN) may stop forwarding packets for PDPs that are configured for the “network behind mobile” feature after a failover.

Conditions: This issue is seen only for “network behind mobile” PDPs after a failover.

Workaround: There is no workaround.

- CSCsv97424

Symptoms: Router crashes due to memory corruption in the I/O pool. In all of the crashes previous block pointer is corrupted.

Conditions: This symptom is observed in a Cisco 2811 that is running Cisco IOS Release 12.4(22)T.

Workaround: There is no workaround.

- CSCsy30256

Symptoms: A Cisco 2811 router crashes due to a bus error after an ISDN call terminates. The following is seen before the crash:

```
%ALIGN-1-FATAL: Corrupted program counter
pc=0x0 , ra=0x400ABA78 , sp=0x44647440
```

```
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x0
```

Conditions: The symptom is observed when “dialer rotary-group *number*” is configured on the interface.

Workaround: Use “dialer pool” instead of “dialer rotary”.

- CSCsy85375

Symptoms: The asynchronous interface of the V.92 modem in a Cisco 1800/890 series router reports input CRC and abort errors when connected with a PVDM2-DM modem module and using V.44 compression. This issue can cause data packet loss.

Conditions: This issue occurs when a V.92 modem which is built in a Cisco 1800/890 series router connects to PVDM2-xxDM modems and is connected with V.44 compression. If V.44 compression is not negotiated, this issue will not occur.

Workaround: Disable the V.44 compression by configuring the 1800/890 modem to negotiate V.42bis by using the below mentioned modemcap. Also, you need to override the system default chat-script with your own, as the system default chat-script will issue the **ATZ** command, which will do a reset of modem, thus the modemcap settings will be lost.

```
1811 V.92 modemcap:
modemcap entry V.42bis:MSC=&FN4%C0+DS=3
```

Sample chat-script:

```
Chat-script dial "" "ATDT" TIMEOUT 60 CONNECT p
```

Sample line configuration to apply the above chat-script.

```
line 1
script dialer dial
modem InOut
no exec
transport input all
transport output all
stopbits 1
speed 115200
flowcontrol hardware
```

- CSCsz70049
Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the telco side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.
Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.
Workaround: Issue the **clear interface bri** command to restore this state.
- CSCta06451
Symptoms: Memory leak is observed in export packets when both OER and Netflow are enabled.
Conditions: The symptom is observed only when both Netflow and OER export is enabled. OER export is enabled by default to a 3949 port.
Workaround: There is no workaround.
- CSCta08870
Symptoms: A memory leak can occur in the VTSP process, due to calls failing to clear completely.
Conditions: The symptom is observed with the VTSP process.
Workaround: There is no workaround.
- CSCta13745
Symptoms: VM notifications sent from CUE to CME SIP trunk may have no audio.
Conditions: The symptom is observed with a SIP trunk and VM notifications sent to PSTN over the SIP trunk.
Workaround: There is no workaround.
- CSCta28282
Symptoms: The Null0 route advertised via VPNv4 flaps.
Conditions: The issue is seen on a Cisco 7200 series router with the Cisco IOS interim Release 15.0(1)M1.10 image
Workaround: There is no workaround.
- CSCta42633
Symptoms: Ping fails to a directly-connected router after removing “frame-relay payload-compression”.
Conditions: The symptom is observed only if “frame-relay payload-compression” is removed on both the routers connected back-to-back.
Workaround: Remove and re-apply the frame-relay map-class under the interface on both the routers connected back-to-back.
- CSCta55561
Symptoms: Per-VRF dampening is not supported.
Conditions: The symptom is observed during normal code flow.
Workaround: There is no workaround.
- CSCta58068
Symptoms: During BGP convergence, CPU spike may be seen on the local PE in an MVPN configuration after conditions.

Conditions: Conditions causing excessive BGP convergence and high CPU utilization (with and without traffic) in an MVPN setup can be varied as:

- Remote PE neighbor switchover
- On local PE, do a **clear ip bgp nbr**.
- On bringup of local PE
- Large configuration such as one with 300 MDT default tunnels.

Here is an example of an MVPN configuration where this problem can be exhibited:

1. OSPF routing protocol is enabled on all the networks in the topology.
2. Each PE router has 100 MVRFs defined (between vpn_0 to vpn_99)
3. MDT default is configured on all the mVRFs on the PE routers
4. PE routers have an iBGP session, ONLY with the RR (route-reflector)
5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes
6. OSPF session also exists between Routem and PE1, with Routem sending 100 OSPF routes

In effect the following states are present in the network:

On PE and RR routers:

1. IGP states = 100 OSPF routes
2. BGP states = 200,010 VPNv4 routes

On PE routers ONLY:

1. VRF sessions = 100 VRFs (vpn0 to vpn_99)
2. MDT sessions = 100 SSM sessions

Workaround: There is no workaroun.

- CSCta78212

Symptoms: Following an upgrade to Cisco IOS Release 12.4(15)T7 with IPS v5, there is a severe drop in throughput for customer traffic when IPS is enabled.

Conditions: The symptom is observed with the following conditions:

- A Cisco 1841 router that is running Cisco IOS Release 12.4(15)T7.
- The image is c1841-advsecurityk9-mz.124-15.T7. - IPS v5.

Workaround: Deactivate IPS from interface.

- CSCtb26941

Symptoms: Intermittent echo on voice calls are experienced. All calls through a particular DSP channel will experience echo.

Conditions: The symptom is observed when a DSP channel, or set of DSP channels, go into a bad state where they no longer cancel echo. The audio stream coming into the DSP will match exactly what is going out. This can be identified by the symptom that the echo-cancellation tail will vary during a call even when the tail is specified on the voice port. Values from 24ms to 112ms have been observed for a single call which this issue occurs on. The **show call active voice echo-canceller summary** command can be used to observe the echo cancellation tail, and the voice-port command **echo-cancel coverage** can be used to statically set the echo cancellation tail.

Workaround: The DSP can be reset, or the gateway can be reloaded, and the echo canceller will begin functioning.

- CSCtb38071

Symptoms: While testing the Large-Scale Dial-Out (LSDO) feature, the expected number of links is not seen in the bundle after starting calls in both directions for a single client. The traffic is sent for around 10 minutes. Dialer map is formed for the required address.

Conditions: This issue is seen in a router that is loaded with Cisco IOS interim Release 12.4(24.6)PI11r.

Workaround: There is no workaround.

- CSCtb39756

Symptoms: New GM is not able to communicate to existing GMs.

Conditions: The symptom is observed under the following conditions:

1. Primary keyserver reloads.
2. Secondary keyserver takes over role as primary and removes the old TEK and creates a new TEK2.
3. During the period where the existing GMs have both old and new TEK keys, any new GM that registers will only get the new TEK. This new GM will not be able to communicate to the existing GMs until the old TEK expires.

Workaround: There is no workaround.

- CSCtb42862

Symptoms: A Cisco 3845 router crashes due to illegal memory access.

Conditions: The symptom is observed in a scale testing environment which has eight key servers and 20 GM routers (simulating 2000 group members) and when there is unicast rekeying. The GM router crashes in steady state (no traffic). This seems to be intermittent.

Workaround: There is no workaround.

- CSCtb47647

Symptoms: Active RP crashes at pim_send_join_prune, when starting memory leak debugging and after executing the **show memory traceback exclusive** command.

Conditions: To be determined.

Workaround: There is no workaround.

- CSCtb51244

Symptoms: Spurious memory access is seen when deleting a policy map.

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(24.6)PI11u.

Workaround: There is no workaround.

- CSCtb55576

Symptoms: When a HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

Workaround: There is no workaround.

- CSCtb67800

Symptoms: Memory leak is observed when zone-based firewall policy is configured and unconfigured.

Conditions: The symptom is observed on a Cisco 7200 series router.

Workaround: There is no workaround.
- CSCtb98159

Symptoms: TCP connections made to the IP address of an interface on a Cisco 870 router are dropped when “IPSec VPN” and “protocol inspection” are configured for the same interface. TCP connections that are dropped are not made over an IPSec connection.

Conditions: The symptom is observed under the following conditions:

 - IPSec VPN is configured for the interface.
 - Inspection is configured for the interface with the **ip inspect** command.

TCP drops are triggered by a successful IPSec VPN session establishment and termination to the interface.

Workaround: There is no workaround.
- CSCtb99736

Symptoms: ISDN cause codes are not being forwarded transparently to the PBX.

Conditions: The symptom is observed with a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T1. It is seen when the ISDN interface is configured with “isdn global-disconnect” on both sides.

Workaround: There is no workaround.
- CSCtc06935

Symptoms: Packet loss occurs between two Cisco Catalyst 3200 MAR routers connected over FESMIC Fast Ethernet ports via wireless radios after upgrading to Cisco IOS Release 12.4(22)T2.

Conditions: The symptom is observed with the following conditions:

 - After a code upgrade.
 - On Cisco Catalyst 3200s connected via wireless radios.
 - It does not occur on devices directly connected via fiber.

Workaround: Use Cisco IOS Release 12.4(1a).
- CSCtc12002

Symptoms: An NM-1A-OC3-POM can not achieve line rate. Router performance degradation is observed.

Conditions: The symptom is observed with an NM-1A-OC3-POM module on a Cisco 3945 router. The performance degradation issue is observed for OC3 module while trying to reach OC3 line rate with small size (64Bytes) bi-directional traffic streams. Non-drop rate and CPU utilization performance is degraded due to this issue.

Workaround: Avoid touching line rate with small size bi-directional traffic streams (uni-directional traffic can touch line rate without any problem).
- CSCtc28073

Symptoms: Packets are dropped when VPDN is configured as there are two IP headers added to the packet.

Conditions: The symptom is seen when VPDN is configured and CEF is enabled.

Workaround: Disable CEF.

- CSCtc33476

Symptoms: The UUT crashes.

Conditions: The symptom is observed when running IPv6 inspection. The issue is seen with IPv6 FTP inspections.

Workaround: There is no workaround.

- CSCtc38922

Symptoms: A router crashes when “ip inspect” is configured.

Conditions: The symptom is observed when “ip inspect” is configured.

Workaround: Disable “ip inspect”.

- CSCtc42605

Symptoms: Memory leak can be observed when reconfiguring class-map attached to a zone-pair.

Conditions: The symptom can be observed with a router that is running Cisco IOS Release 15.0(1)M0.1.

Workaround: There is no workaround.

- CSCtc45177

Symptoms: The “text_start” is not showing up in crashinfo.

Conditions: The symptom is observed with crashinfo data.

Workaround: There is no workaround.

- CSCtc45487

Symptoms: On a random set of dVTI spokes, IPSec tunnels get randomly stuck. The tunnel interface on the spoke(s) goes down (administratively UP, line protocol DOWN). Traffic does not pass anymore although the crypto socket shows “UP”, crypto is up, and all looks ok, except for the line protocol is down.

The matching virtual-access on the hub stays up. The crypto is still up and running (DPD is working and even rekey).

Conditions: The symptom is observed with the following conditions:

- (dVTI) terminating a large set of tunnels.
- IPSec tunnel protection.
- Cisco IOS Release 12.4(15)T9.

Workaround: Do a shut/no shut of the affected tunnel interfaces.

- CSCtc59535

Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

Workaround: Unplug and plug back the cable.

- CSCtc68910

Symptoms: Unnecessary retransmission and spurious TCP is reset.

Conditions: The symptom is observed when using NAT and a large (already fragmented) “updatecapabilitiesversion2” traverses the router.

Workaround: There is no workaround.

Further Problem Description: This problem seems to be correlated to:

- IP phone presents an updatecapabilitiesversion2 large packet (i.e.: 2012 bytes) fragmented (i.e.: in 4 pieces).

- CSCtc71408

Symptoms: Fax transmission fails when CUBE is in the middle.

Conditions: The symptom is observed when either one of the dial-peers on OGW/TGW/CUBE is configured for fax protocol T38 version 0.

Workaround: Configure version 3 on all dial-peers.

- CSCtc79092

Symptoms: Timeout of active connections.

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T1 and Release 12.4(22)T1 with ZBF enabled. The issue only occurs for TCP connections when using ZBF, and is most noticeable for RDP connections. Problem is not seen when ZBF is not configured on the interface and is present even when crypto configuration is not present.

Workaround: There is no workaround.

Further Problem Description: The output of **show policy-map type inspect zone-pair session** suggests that for single traffic stream (RDP stream) two sessions are created. One session is in half open state the other is fully established. By default the idle-timeout for half-open session is 30 sec, so after 30 seconds the half-open session is deleted and along with that it also deletes the established session.

For both match protocol and match access-group based inspection, when inspecting TCP based protocols, inspection mechanism creates duplicate sessions.

- CSCtc82516

Symptoms: The inbound ACL applied on the GRE tunnel interface is bypassed.

Conditions: The symptom is observed when CEF switching is turned on. The crypto ACL encrypts all traffic going through this GRE tunnel. The ACL is trying to filter out some specific host, and is applied inbound.

Workaround: There is no workaround.

- CSCtc87330

Symptoms: Periodically, you may get bad “getbuffers” in “IP Input” process.

Conditions: The symptom is observed when running traffic overnight.

Workaround: There is no workaround.

- CSCtc90459

Symptoms: Inbound ACL is not working properly. It does not allow packets to pass that should.

Conditions: The symptom is observed when you configure “input access list” to allow voice packets (SIP protocol). If you apply the following configuration on the router the voice packets will get dropped:

```
access-list 101 permit udp host 85.38.230.34 eq 5060 host 85.34.23.74
access-list 101 permit udp host 85.38.230.34 host 85.34.23.74 range 16384 32767
```

- Workaround: Use “log” keyword at the end of the ACL.
- CSCtd02018

Symptoms: Unable to pass traffic.

Conditions: The symptom is observed with IPv6 DMVPN (tunnel protection), IPv6 inspect, and IPv6 CEF.

Workaround 1: Use running in process.

Workaround 2: Take the tunnel protection off.

Workaround 3: Use the **no ipv6 inspect** command.
 - CSCtd10824

Symptoms: Switch occasionally crashes when power is turned off on an interface using the **energywise** command.

Conditions: It occurs when recurrences are already set on the interface and if they are in effect.

Workaround: Use “energywise” queries to set levels on the interface. Queries is a more robust and time-saving technique to set levels on interfaces in bulk.
 - CSCtd12681

Symptoms: Misordered packets occur among packets which belong to the same class-map when shaping becomes active on the tunnel interface.

Conditions: The symptom is observed under the following conditions:

 1. IPSec must be enabled, either on tunnel or physical interface.
 2. Shaping (with either **bandwidth** or **priority** command) must be applied on tunnel interface.
 3. There should be enough traffic to trigger shaping.
 4. On a Cisco 7200 series router, VAM2+ or software encryption engine has to be used.

Workaround: Use Cisco IOS Release 12.3(14)T2 or earlier, and crypto map on physical interface instead of tunnel protection on tunnel interface for IPSec encryption.

Alternate Workaround: Use Cisco IOS Release 12.4(20)T or later where HQF QoS is introduced. HQF QoS does not have the issue regardless of hardware or software configurations.
 - CSCtd12700

Symptoms: A GM pseudotime gets desynchronized after re-registering or at initial registration.

Conditions: The symptom is observed with GETVPN when Time Based Anti-Replay (TBAR) is enabled. After establishing phase I, the GM is supposed to get the KEK and TEKs. If there is packet drop (most of the time this message is fragmented across multiple frames), then the router is not able to reassemble the packet. Then IKE will resend this message later but the pseudotime has not been recalculated.

Workaround: Disable TBAR or use a very large window (greater than 30 seconds).
 - CSCtd23069

Symptoms: Crash due to SegV exception after configuring “ip virtual-reassembly”.

Conditions: The symptom is observed on a Cisco 7206VXR router configured as LNS that is running Cisco IOS Release 12.4(15)T7 and Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd25879

Symptoms: When upgrading to Cisco IOS Release 12.4(15)T10, IPSec client can connect to a Cisco 7301 router but when the IPSec client disconnects, the router keeps the IPSec session UP. It is not possible to connect to the 7301 IPSec concentrator again.

Conditions: The symptom is observed with a Cisco 7301 router that is running Cisco IOS Release 12.4(15)T10.

Workaround 1: Disable/enable crypto map:

```
interface gig 0/0
no crypto map
crypto map map name
```

Workaround 2: Remove access-list and apply again:

```
interface gig 0/0
no ip access-group ACL NAME in
ip access-group ACL NAME in
```

Workaround 3: Reload the router.

- CSCtd28809

Symptoms: An HWIC-3G may not work on some sites. The following error messages may be seen:

```
CELLWAN-2-HEART_BEAT_TIMEOUT: No heart beat signal from Cellular0/1/0
HWIC_CELL-1-MODEM_ACK_FAIL : [Cellular0/1/0] Modem Ack not received
```

Conditions: The symptom is observed on a Cisco 1841 router.

Workaround: Use the following steps:

- Power off the router.
- Disconnect the cable from the antenna.
- Power on the router.
- Wait until you have the prompt on your console or when you can access it via telnet.
- Screw antenna cable back.

At this point, communication should be possible.

- CSCtd34862

Symptoms: The command **show policy-map interface *multilink1***, shows that transmitted packets/bytes counter is incorrectly increasing for DSCP values that is not being matched in the class map on the Cisco 2821 platform.

Conditions: The symptom is observed on a Cisco 2821 router.

Workaround: There is no workaround.

- CSCtd37738

Symptoms: The symptoms are as follows:

- Phone A calls Phone B.
- Phone B is call-forwarded to a cell phone C.
- Cell phone C is ringing.
- Phone A does not hear ring back.

Conditions: The symptom is observed when the CCM is between CUBE and VGW.

Workaround: There is no workaround.

- CSCtd42508

Symptoms: PVDm3 DSP might crash under excessive T38 fax call failures.

Conditions: This symptom is observed under network packet loss conditions.

Workaround: There is no workaround.

- CSCtd57788

Symptoms: A dynamic IP ACL is created when a session comes up and is together with the policy private route created according to the “Ascend-Private-Route” downloaded from the user profile. When the session goes down, the route is cleared but the dynamic ACL is not cleared:

```
dge2-18#sh ip access-lists dynamic
Extended IP access list pbr#1
    10 permit ip any host 10.1.1.1 (5 matches)
Extended IP access list pbr#2
    10 permit ip any host 10.1.1.1 (5 matches)
Extended IP access list pbr#3
    10 permit ip any host 10.1.1.1 (25 matches)
Extended IP access list pbr#4
    10 permit ip any host 10.1.1.1 (25 matches)
Extended IP access list pbr#5
```

Conditions: The symptom is observed with routes downloaded from the radius server.

Workaround: There is no workaround.

- CSCtd59027

Symptoms: The device crashes due to a bus error.

Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCtd61443

Symptoms: GETVPN key server may crash after modifying group ACL.

Conditions: This is seen on Cisco router with Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd64434

Symptoms: FastEthernet port on a NM-2FE2W stops processing incoming packets.

Conditions: The symptom is observed with an NM-2FE2W Network Module.

Workaround: There is no workaround.

- CSCtd73843

Symptoms: A Cisco 1801 router flaps intermittently.

Conditions: The symptom is observed with a third-party vendor IP DSLAM.

Workaround: There is no workaround.

- CSCtd75189

Symptoms: Continuous error message similar to the one below are recorded on voice gateway:

```
SYS-2-INPUTQ: INPUTQ set, but no IDB, ptr=6818DA34, -Traceback=
```

Conditions: The symptom is observed on a voice gateway that is running Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd79357

Symptoms: Issuing the **show license call-home pak xxx** command at TCL mode will crash system. For example:

```
Router(tcl)#exec "show license call-home pak PAKString"
```

Conditions: The symptom is observed upon issuing the **show license call-home pak xxx** command at TCL mode.

Workaround: There is no workaround.

- CSCtd86638

Symptoms: Router reports the following error messages,

```
- %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for CCE 7tuple dyn No
memory available -Process= "Chunk Manager", ipl= 3, pid= 1 -Traceback=
0x232BCB84z 0x232BCB68z
- %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for Firewall State. No
memory available -Process= "Chunk Manager", ipl= 3, pid= 1 -Traceback=
0x232BCB84z 0x232BCB68z
```

Conditions: The symptom is observed when the router has high sessions, i.e.: connections/second coming in for prolonged period of time.

Workaround: There is no workaround.

- CSCtd90030

Symptoms: A Cisco 2851 router may crash with a bus error.

Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd90367

Symptoms: Router crashes every 2-3 days with URLF feature. The error message shows memory leak issues.

Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(24)T2, with URLF features on the device.

Workaround: There is no workaround.

- CSCtd94789

Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCtd95386

Symptoms: An IPsec tunnel can be torn down if the router receives a replayed QM (Quick Mode) packet.

Conditions: This is only a problem when a replayed QM packet is received on an IPsec endpoint.

- Workaround: There is no workaround.
- CSCtd97164

Symptoms: LLQ packet drops on an ATM interface.

Conditions: The symptom is observed when having QoS under an ATM interface. Packet drops are seen under a class with “priority”, even though they have not reached the value configured. It does not matter if it is percent or absolute value.

Workaround: There is no workaround.
 - CSCte01576

Symptoms: CPU goes up to 99 percent when TRP is used for making voice calls with 50 SCCP and 50 SIP endpoints.

Conditions: The symptom is observed when STUN inspection is enabled on the firewall for media traversal.

Workaround: Use SIP or SCCP inspection.
 - CSCte02973

Symptoms: Routing protocols like EIGRP may be dropped in the global table.

Conditions: The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

Workaround: Enable “ip multicast routing” and create a loopback interface with “ip pim sparse-mode” enabled.

Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.
 - CSCte03048

Symptoms: Fragmentation does not occur on a Cisco 7200 series router.

Conditions: The symptom is observed when FR encapsulation is configured and fragmentation is enabled. Now do a **wr mem** and reload.

Workaround: Perform an OIR on the PA.
 - CSCte07401

Symptoms: Normal mode GD fails with tracebacks when you execute the **show memory debug leak chunks** command.

Conditions: This symptom is seen when you check for memory leaks after clearing an L2TP session.

Workaround: Wait for all sessions to tear down and then check for leaks.
 - CSCte07862

Symptoms: DSP crashes due voice card shutdown, with an intermittent CPHI error.

Conditions: The symptom is observed when the phones are connected to PBX. Users dial 5XXXX from the phone. The pattern then changes to 895XXX between PBX and the Cisco router. Over the IP, the call is transferred to 2821 voice card gateway where there is another PBX.

Workaround: There is no workaround.

- CSCte12104
Symptoms: Crash at startup with the following error message:
%SYS-6-STACKLOW: Stack for process ATM Periodic running low, 0/9000
Conditions: The symptom is observed when QoS policy is applied on an ATM interface. There is no specific trigger.
Workaround: There is no workaround.
Further Problem Description: This issue may not be widely hit as it is difficult to reproduce.
- CSCte16755
Symptoms: In an IPsec GetVPN setup, multicast endpoints are not reachable/pingable.
Conditions: The symptom is observed with Cisco IOS Release 12.4(15)T12.
Workaround: There is no workaround.
- CSCte17284
Symptoms: A router may unexpectedly reload due to software forced crash because of chunk memory corruption.
Conditions: The crash appears to happen when using the clientless web proxy method. The crash is triggered by accessing a webpage through the SSL VPN with a URL longer than 1009 characters long.
Workaround: If possible, redesign the website to use URLs of 1009 characters or shorter.
- CSCte17560
Symptoms: Offered rate in QoS class shows unusually high values
Conditions: The symptom is observed when service-policy is applied on a multilink interface.
Workaround: There is no workaround.
- CSCte18124
Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024”.
Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.
Workaround: Create ATM PVC without “atm vc-per-vp 1024”.
- CSCte27805
Symptoms: Self ping on a dialer interface fails when it is over a PPPoE link.
Conditions: The symptom is observed when the dialer interface is up and its underlying interface is PPPoE.
Workaround: There is no workaround.
- CSCte39643
Symptoms: A router crashes.
Conditions: The symptom is observed with OER and EIGRP configurations.
Workaround: There is no workaround.
- CSCte41231
Symptoms: Router crashes when unconfiguring “iphc profile”.

Conditions: The symptom is observed when “iphc profile” is configured on dialer interfaces. Then “iphc profile” is not properly removed from the dialer followed by a “no iphc-profile” done globally.

Workaround: There is no workaround.

- CSCte51958

Symptoms: Large amount of memory leaks are seen at Expression Handler.

Conditions: The symptom is observed while doing an SNMP set and walk on expExpressionEntry table.

Workaround: There is no workaround.

- CSCte53097

Symptoms: When the IP address of the HA is set to the VIP address of HSRP, end-to-end connectivity will be lost. Tunnel keepalives from the mobile node fail and the bindings are deleted from HA.

Conditions: This is seen in Cisco IOS Release 12.4(23) when using the HA behind a NAT device and the translated (inside) IP of the HA is set to the HSRP VIP address.

Workaround: Configure a loopback interface (does not have to be routed) with the same outside (public) IP that the mobile node connects to. This is the outside IP defined in the NAT rule on the NAT device.

- CSCte53275

Symptoms: A Cisco 1841 router running GETVPN with Cisco IOS Release 15.0(1)M may receive the following error:

```
%SYS-2-SHARED: Attempt to return buffer with sharecount 0, ptr= 667BAEA4
-Process= "Crypto Support",
  ip1= 4, pid= 225 -Traceback= 0x6162E284z 0x631AB270z 0x63342F14z 0x62757380z
0x62757364z
```

Conditions: The exact trigger has not yet been determined.

Workaround: There is no workaround.

- CSCte54807

Symptoms: Configuring PVC with Cisco IOS Release 15.0(1)M1 brings up a virtual-access interface, right after sending the ConfReq, even if there is no reply.

Conditions: The symptom is observed when using a PPPoA setup on Cisco IOS Release 15.0(1)M1. It is seen only if some unused ATM PVCs are present at one end with the PPP configurations applied on them.

Workaround: Use Cisco IOS Release 12.4(24)T2.

- CSCte57140

Symptoms: Lawful intercept does not work for PSTN hairpinned calls. Softswitch redirects the incoming PSTN call to the telco. Although CRCX comes with “L: e:off” and NOT with “L: e:off,nt:LOCAL”, the DSPs are still dropped for the first call.

Conditions: The symptom is observed with a Cisco AS5350XM that is running Cisco IOS Release 12.4(23).

Workaround: There is no workaround.

- CSCte58825

Symptoms: There is a crash upon conducting an snmpwalk from “enterprise mib oid 1.3.6.1.4.1”.

Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 12.2(33)XNE.

Workaround: Configure SNMP view to exclude ipSecPolMap as follows:

```
snmp-server view view name iso included
snmp-server view view name ipSecPolMapTable excluded
snmp-server community community string view view name RO
```

- CSCte61495

Symptoms: The following messages are seen with tracebacks:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process
= Exec. %SYS-2-INTSCHED: 'suspend' at level 3
-Process= "Exec", ipl= 3, pid= 128,
```

Conditions: The symptom is observed when a large ACL is configured for the service-policy. This happens only under ATM subinterfaces.

Workaround: Use small sized ACLs for the service-policy.

- CSCte61528

Symptoms: Router crashes when configuring “tftp hostname” with a longer name.

Conditions: The symptom is observed with a Cisco 7200 series router loaded with the 151-0.25.T image.

Workaround: There is no workaround.

- CSCte62190

Symptoms: A router crashes when the RSA key is generated with redundancy option and then the RSA key pair is deleted using the **crypto pki zeroise rsa** command.

Conditions: The symptom is observed with a router loaded with the c7200-adventerprisek9-mz.151-0.25.T image.

Workaround: There is no workaround.

- CSCte63156

Symptoms: Router hangs and crashes when a DHCP pool configured with “origin aaa subnet” is removed.

Conditions: The symptom is observed when pool is configured with “origin aaa subnet ...” and without unconfiguring this command, the pool is deleted with the **no ip dhcp pool** command. Also missing is “aaa accounting” with “default method-list” from global configuration.

Workaround: Globally configure “aaa accounting” with “default method-list” (“aaa accounting network default”).

- CSCte63390

Symptoms: Memory leak seen under CCH323_CT process. The leak leads to a low memory condition and malloc failures under the processor memory pool.

Conditions: Unknown at this point.

Workaround: There is no workaround.

- CSCte63404

Symptoms: Fax passthrough between H.323 gateway (registered with CUCM 7.1.3) fails.

Conditions: The symptom is observed when CUCM 7.1.3 does the call control for the H.323 gateway. The fax call from GW1 to GW2 gets disconnected as soon as the call is established.

- Workaround: There is no workaround.
- CSCte64544

Symptoms: Calls fail following hook flash on a T1-CAS circuit.

Conditions: The symptom is observed following outbound calls over a T1-CAS E&M, and after a hookflash.

Workaround 1: Reorder circuits in CUCM RG.

Workaround 2: Perform a shut/no shut on the T1-CAS controller.
 - CSCte64621

Symptoms: VSA stops passing traffic after the first IPSec rekey.

Conditions: The symptom is observed VSA specific.

Workaround: There is no workaround.
 - CSCte68288

Symptoms: Spurious memory access is seen when a set of configurations is placed under “crypto pki trustpoint *name*”.

Conditions: The symptom is observed when the router is loaded with the c7200-adventerprisek9-mz.151-0.25.T image.

Workaround: There is no workaround.
 - CSCte68795

Symptoms: High CPU utilization is observed with IP NBAR protocol discovery.

Conditions: The symptom is observed when enabling “ip nbar protocol discovery”.

Workaround: WINMX PDLM needs to be reverted back to the previous version.
 - CSCte70409

Symptoms: A crash seen when running TCL scripts/testcases testing COOP feature of GETVPN.

Conditions: The symptom is observed when running multiple testcases at a time as part of internal testing.

Workaround: There is no workaround.
 - CSCte75220

Symptoms: Router crashes when configuring “key-string www” in key chain mode.

Conditions: The symptom is observed when configuring “key-string www” in key chain mode via console, and when key chain is unconfigured in the vty mode.

Workaround: There is no workaround.
 - CSCte76092

Symptoms: Cisco 880 series router does not write crashinfo.

Conditions: The symptom is observed with a Cisco 880 series router.

Workaround: Connect a device to monitor the console.
 - CSCte76513

Symptoms: If ZBF and WAAS are configured on a router, you may see drop logs similar to the following:

```
%FW-6-DROP_PKT: Dropping tcp session x.x.x.x y.y.y.y due to No zone-pair between zones with ip ident 0
```

%FW-6-DROP_PKT: Dropping http session x.x.x.x y.y.y.y on zone-pair admin-to-wan class admin due to Invalid Flags with ip ident 0

Conditions: The symptom is observed if ZBF and WAAS are configured on a router.

Workaround: There is no workaround.

- CSCte76760

Symptoms: A router acting as a voice gateway may unexpectedly reload due to bus error.

Conditions: The symptom is observed when the gateway is experiencing a low memory problem leading to seeing SYS-2-MALLOCFAIL errors.

Workaround: Resolve the low memory problem.

- CSCte78204

Symptoms: Vaccess interface does not come up.

Conditions: The symptom is observed when **clear interface virtual-access #** is issued on a Cisco 7200 series router and when LFIoFR is configured.

Workaround: Perform a shut/no shut on the serial member.

- CSCte82086

Symptoms: A Cisco 1900 series or Cisco 2900 series router sometimes does not respond to “break” on the RJ45 console or the USB console.

Conditions: The symptom is observed on a Cisco 1900 series or Cisco 2900 series router.

Workaround: Press “break” on the terminal keyboard couple times after seeing “program load complete,...” message, in order to put the router into ROMMON.

- CSCte85781

Symptoms: Policy with more bandwidth than physical and tunnel interface bandwidth is attached on tunnel interface.

Conditions: The symptom is observed with a Cisco 7200 series router and Cisco IOS interim Release 15.1(00.26)T.

Workaround: There is no workaround.

- CSCte85818

Symptoms: Priority burst on **sh policy-map int** shows more than the burst value defined on the command syntax range.

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(00.26)T.

Workaround: There is no workaround.

- CSCte89130

Symptoms: Router experiences a memory leak.

Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).

Workaround: There is no workaround.

- CSCte89436

Symptoms: Router crashes.

Conditions: The symptom is observed when encapsulation is changed from “frame-relay” to “hdlc”.

Workaround: There is no workaround.

- CSCte89787

Symptoms: A Cisco ASR 1000 crashes after the Segment Switch Manager (SSM) reports that an invalid segment has been detected:

```
%SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment class.
```

The crash follows this message.

Conditions: The symptom is observed on a Cisco ASR 1002 that is running Cisco IOS Release 12.2(33)XND1. The crash is caused by a NULL pointer de-reference following the “no segment class” error. The error itself is not fatal and the crash should have been avoided.

Workaround: There is no workaround.

- CSCte90278

Symptoms: Watchdog crash observed on a Cisco 3845 router.

Conditions: The symptom is observed with a Cisco 3845 router with frame relay encapsulation on the dialer and WIC-1DSU-T1-V2 serial interfaces.

Workaround: There is no workaround.

- CSCte91471

Symptoms: Clock synchronization with the NTP server could be lost for several hours if router (NTP client) runs NTPv4.

Conditions: The symptom is observed if the router clock is reset (for example: by using the **clock set** exec command). The router then takes a long time to synchronize again.

Workaround: There is no workaround. The clock will automatically synchronize after few hours.

- CSCte91782

Symptoms: Cannot unconfigure “crypto pki server <>” when “crl” is configured.

Conditions: The symptom is observed on a router loaded with Cisco IOS interim Release 15.1(1.1)T.

Workaround: There is no workaround.

- CSCte91990

Symptoms: A Cisco 3845 router with HWIC-4ESW is flooding packets to all interfaces even back across the same interface.

Conditions: The symptom is observed when sending to a packet with a multicast MAC and unicast IP address.

Workaround: There is no workaround.

- CSCte93792

Symptoms: Virtual access bound to an ATM interface does not come up.

Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.

Workaround: There is no workaround.

- CSCte94221

Symptoms: PPP connection over CDMA link is flapping.

Conditions: The symptom is observed when using Cisco IOS Release 15.0M.

Workaround: There is no workaround.

- CSCte95301

Symptoms: Memory leak in proxy authentication scenario, when authentication fails.

Conditions: The symptom is observed when HTTP proxy authentication is used.

Workaround: There is no workaround.

- CSCte98702

Symptoms: When using NAT, “%SYS-3-INVMEMINT and %SYS-2-MALLOCFAIL” are printed to the console and no traffic passes.

Conditions: The symptom is observed when NAT is configured.

Workaround: There is no workaround.

- CSCtf00427

Symptoms: A router may experience a severe memory leak issue when the following command is configured:

privilege exec level level show ip ospf neighbor

Conditions: The symptom is observed when running Cisco IOS Release 12.2(33)XNE or 12.2(33)XNE1. The issue is not platform dependent.

Workaround: Reload the router.

- CSCtf03436

Symptoms: A two-level policy attached on a multilink interface is getting detached when the interface undergoes a shut/no shut.

Conditions: The symptom is observed with a two-level policy configured with shaper/bandwidth percent. It is seen on a Cisco 7200 series router.

Workaround: There is no workaround.

- CSCtf03850

Symptoms: The **configure replace**/**terminal revert** commands are not working.

Conditions: The symptom is observed on a Cisco 2811 router that is running Cisco IOS Release 15.0(1)M and a Cisco 877W router that is running Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

- CSCtf04132

Symptoms: Tracebacks are seen on an L2TP Network Server (LNS) after new session is established.

Conditions: The symptom is observed on an LNS.

Workaround: There is no workaround.

- CSCtf05429

Symptoms: Serial interface flap is seen on a Cisco 7200 series router.

Conditions: The symptom is observed when controller 1/1 is configured as unchannalized and then you do a sweep ping.

Workaround: There is no workaround.

- CSCtf07474

Symptoms: TCP sessions fail to establish between two routers over an IPSEC VPN tunnel after an EZVPN client session has been established and torn down to the two routers. The TCP sessions could be a telnet or H.323 sessions that terminate and originate between the two routers. Logs show:

```
%FW-6-DROP_PKT: Dropping tcp session 192.168.10.1:58553 192.168.20.1:23 due to
Invalid Segment with ip ident 35331 tcpflags 0x5010 seq.no 2978402186 ack 1370657297
```

Conditions: The symptom is observed under the following conditions:

- Two routers setup with IPSEC point-to-point VPN.
- Using Cisco IOS Release is 15.0(1)XA or later.
- Both routers are setup as EZVPN servers.
- An EZVPN session has been established to one of the routers and has been disconnected.

Workaround:

- Always keep an EZVPN client session up to the router.
- Remove and add **ip inspect** on WAN interface after EZVPN session has been disconnected.

- CSCtf08645

Symptoms: A Cisco 2800 series router crashes.

Conditions: The symptom is observed with the c2800nm-advipservicesk9-mz.124-24.T2 image. The crash is most likely to occur when a hardware IDS module is present.

Workaround: There is no workaround.

- CSCtf09228

Symptoms: A router may crash.

Conditions: The symptom is observed on a Cisco 1802W router that is running Cisco IOS Release 15.0(1)M1, after bringing up a second PPPoE connection.

Workaround: There is no workaround.

- CSCtf11642

Symptoms: A router may crash due to a bus error.

Conditions: The symptom has been observed on a Cisco 1841 router that is running Cisco IOS Release 12.4(24)T2, with IOS Firewall configured.

Workaround: There is no workaround.

- CSCtf13014

Symptoms: DNS server on a router first consults with its next-level DNS servers when servicing queries for its primary zone.

Conditions: This symptom only happens when next-level (parent) DNS servers are configured on the router.

Workaround: There is no workaround.

- CSCtf13408

Symptoms: Router crashes when using “config replace” to remove “sccp” configurations such as “associate ccm” and “associate profile” in the “sccp ccm group” sub-mode.

Conditions: This symptom occurs when SCCP is enabled and configured with “associate ccm” or “associate profile”, and “config replace” is used to roll back the router configuration to a state where “associate ccm” or “associate profile” for “sccp ccm group” does not exist, i.e. to remove those configuration commands after rollback.

Workaround: The user can manually change the configuration instead of using “config replace” as follows:

1. Use the command **show archive config differences [flash: | file path]** to determine the difference between the running-config and the saved config (in flash: or by valid file path);
 2. Manually change the running config line-by-line through the differences shown in the above command output.
- CSCtf18077
Symptoms: A CME router may unexpectedly reload due to bus error when a UCCX unregisters from the CME.
Conditions: This symptom is seen when the UCCX unregisters from the CME.
Workaround: There is no workaround.
 - CSCtf19461
Symptoms: IP address is not leased out to the client from server.
Conditions: Configuring vpn sub-option at the interface level on relay
Workaround: There is no workaround.
 - CSCtf19572
Symptoms: Crash occurs while unconfiguring “interface ATM0/1/0.1 point-to-point”.
Conditions: This symptom is observed while unconfiguring “interface ATM0/1/0.1 point-to-point”.
Workaround: There is no workaround.
 - CSCtf22064
Symptoms: Invalid configuration is attaching on frame relay map class
Conditions: This symptom is observed on a Cisco 7200 platform on Cisco IOS interim Release 15.1(1.3)T
Workaround: There is no workaround.
 - CSCtf22377
Symptoms: A Cisco 2851 reboots due to bus error, packets (skinny) leaking
Conditions: This crash is due to a buffer leak in the small buffers
Workaround: There is no workaround.
 - CSCtf23119
Symptoms: On a connection trunk circuit that has it voip dial peers configured for dtmf-relay rtp-nte, dtmf stops working, where it is not heard on the receiving tdm circuit. With debug voip rtp session name-event enabled you still see rtp-nte debugs being received on the terminating side gateway, but no digits are heard on the tdm side out of the dsp.
Workaround: A shut / no shut of one of the voice ports will drop and reconnect the connection trunk circuit and dtmf-relay rtp-nte will again work.

- CSCtf25009

Symptoms: Multicast traffic sent out of a GE-DCARD-ESW on a NM-16ESW is process-switched, instead of being fast-switched.

Conditions: This symptom is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(25b).

Workaround: Use the onboard Gigabit interface.

- CSCtf25131

Symptoms: Router crashes.

Conditions: This symptom is observed when a large number of ISG sessions [27K or more] go down simultaneously while there is a CPUHOG on the box. Check for memory leaks using the **sh mem debug leaks chun** command.

Workaround: Do not try to check for memory leaks in case there is a CPUHOG on the box.

- CSCtf25508

Symptoms: Customers are not able to remove isakmp profiles followed by the error msg “% Profile is applied to Virtual-Access2-head-0/65536 and possibly other crypto maps”.

Note where 2 is in the Error msg will differ based on the customers configuration. In the above message Virtual-Access 2 is reference because the VTI number in this case was 2.

This also keeps many stale dynamic crypto map entries without any valid ipsec sa or virtual access interface.

Conditions: This symptom is seen when using VTI with EZVPN and only seen in Cisco IOS Release 12.4(24)T.

Workaround: Reload the Router to release hung Virtual-Access Sessions

- CSCtf25886

Symptoms: The following messages are observed on the console:

```
028970: Feb 24 18:58:34.565: %C5510-1-NO_RING_DESCRIPTOR: No more ring descriptors
available on slot 5 dsp 13.
```

```
028971: Feb 24 18:58:39.621: %C5510-1-NO_RING_DESCRIPTOR: No more ring descriptors
available on slot 3 dsp 17.
```

```
028972: Feb 24 18:58:44.629: %C5510-1-NO_RING_DESCRIPTOR: No more ring descriptors
available on slot 3 dsp 17.
```

The RST (ReSeT) counter column in the output of the **show voice dsp detail** command will show non-zero values for some Digital Signal Processor (DSP) IDs, indicating that a DSP has reset itself.

Conditions: This behavior may be observed on a Cisco Voice GateWay that is installed with PVDM2 C5510-based DSP cards: PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-48, PVDM2-64, and AS5X-PVDM2-64, and configured for TDM-IP Voice Services. At present this symptom has been observed with Cisco IOS Release 12.4(15)T12 and default DSP firmware version 9.4.12, as well as when DSPware 9.4.10 or 9.4.11 is used in place of 9.4.12.

Workaround: Lab reproduction work has demonstrated that superseding the default DSPware in Cisco IOS 12.4(15)T12 with DSPware version 9.4.9 or earlier constitutes a stable combination of Cisco IOS and DSPware.

- CSCtf27324

Symptom: s Ping from a CPE which is doing PPP to the ip address of the LNS router that terminates that PPP call fails. PPP has been opened, and IPCP has negotiated an IP address. Ping from the LNS back to the CPE works fine. Between the LAC and the LNS there is a PPP multilink bundle.

Conditions: The issue happens only when we have a plain PPP call from a client (ISDN modem or dial up modem which is doing PPP). In addition the physical connectivity between the LAC and the LNS is PPP multilink.

Workaround: Disable cef on the physical interface between the LAC and the LNS. If the CPE is doing PPP multilink ping works fine.

Further Problem Description: The issue seems to be specific with the forwarding of the packets through the PPP multilink bundle that exists between the LAC and the LNS.

- CSCtf28796

Symptoms: With async_dialer interface type, PPP fails.

Conditions: This issue is seen only with async_dialer interface type. There is no issue with async_legacy and async_virtual interface types.

Workaround: There is no workaround.

- CSCtf32094

Symptoms: Traffic drops on the bundle interface with input error.

Conditions: This symptom occurs when one member link is removed.

Workaround: There is no workaround.

- CSCtf32916

Symptoms: Incoming SIP call forwarded to external destination via SIP trunk will be dropped after negotiated session time expires.

Conditions: This symptom is seen in Cisco IOS Release 12.4(24)T1 with forwarded SIP-SIP calls and session timer negotiated (RFC 4028). It is not seen in Cisco IOS Release 12.4(11)XW9.

Workaround: -Disable or increase session timer on SIP trunk(s).

- CSCtf33270

Symptoms: Router crashes while giving shutdown under config-nxg-neigh-svc mode.

Conditions: This symptom is seen on a Cisco 7200 router that is loaded with Cisco IOS Release 15.1(1.4)T image.

Workaround: There is no workaround.

- CSCtf34183

Symptoms: Secondary CM fails to register.

Conditions: This symptom is observed after correcting the user name.

Workaround: There is no workaround.

- CSCtf35006

Symptoms: We have two jobs in SNMP job Q. Try to destroy the jobs and console hangs.

Conditions: This symptom is seen when preparing multiple license action entries and then let them execute immediately.

Workaround: There is no workaround.

- CSCtf36117

Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections

Conditions: The test scenario involves setting up as much as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established, and the CLI is trying to list down the sessions. This problem is reproducible at will.

Workaround: There is no workaround.

- CSCtf36285

Symptoms: Secondary link is not dialed after the expiry of the initial route-check timer

Conditions: The failure is seen only in Cisco IOS Release 12.4(24)T3.

Workaround: There is no workaround.

- CSCtf40731

Symptoms: Routing is formed when PIRO and OER generates static route works together.

Conditions:

1. PIRO generates more specific prefix for the static route it created.
2. OER generates static route redistributed into other IGP protocol in order to get traffic.

Workaround: There is no workaround.

- CSCtf41515

Symptoms: There is an end-to-end ping failure.

Conditions: This symptom is seen with the following topology:

```
7200-a <-----> 3845 <-----> 7200-b
```

After “frame-relay payload-compression” is removed on Cisco 7200-a and Cisco 3845, Cisco 3845 is able to ping Cisco 7200-a, but Cisco 7200-b is not able to ping Cisco 7200-a.

Workaround: There is no workaround.

- CSCtf45586

Symptoms: GW is not playing the remote ringback tone when 180 with SDP is received.

Conditions: This symptom occurs when switching from local ringback tone to remote ringback tone.

Workaround: There is no workaround.

- CSCtf47094

Symptoms: After call connects between Remote phone and HQ, call either has no way or one way audio. Error is observed on the remote CISCO881.

```
*Feb 24 23:30:25.675: %FW-6-DROP_PKT: Dropping tcp session 172.17.10.1:2000
172.16.20.101:50575 on zone-pair ccp-zp-out-self class icmp-self due to Invalid Flags
with ip ident 0
```

Conditions: This only happens if the remote 79xx phone is running 8.x Phone firmware. Remote phone needs to be connected back to HQ via ZBFW and EZVPN

```
CISCO881 using 15.0.1.M1
CME3825 using 15.1.1.XB
CP-7940 using P00308000500
```

Topology:

```
SCCP_7940 Ph1--CISCO881--ZBFW/EZVPN--ASA5520--CME3825--IP phone/PSTN Ph2
```

Workaround: Downgrade phone firmware to a 7.x release.

- CSCtf47335
Symptoms: Wrong typedef version is returned.
Condition: On getTypedefs CT, Cisco IOS returns a typedefVerion “2008-08-01”. This is a wrong version with some undefined entries. Due to this, the signature parsing is failing in CCP.
Workaround: There is no workaround.
- CSCtf47396
Symptoms: Router may crash when a service-policy configured with bandwidth is removed from an interface.
Conditions: This issue is seen with Cisco 7200 router that is loaded with Cisco IOS interim Release 15.1(1.5)T image.
Workaround: There is no workaround.
- CSCtf48094
Symptoms: UUT crashes for ftp traffic with debugs enabled for IPv6 inspection.
Conditions: Crash is seen only with Legacy Firewall for IPv6 inspection.
Workaround: There is no workaround.
- CSCtf48179
Symptoms: When using authentication header only (no encryption over the tunnel) around 30% of outgoing traffic is dropped due to incorrect IP header checksum.
Conditions: This symptom is occurring on 2 different Cisco 2901 routers that are running Cisco IOS Release 15.0(1)M1. AH is configured via “crypto ipsec transform-set AH-MD5 ah-md5-hmac”. This problem occurs only on high latency link (via sitcom).
Workaround: Encrypt the packets by changing the transform-set from ah-md5-hmac to esp-3des esp-sha-mac.
- CSCtf48612
Symptoms: Active learnt forwarder for GLBP should never timeout with a listening forwarder present.
Conditions: Configure GLBP on two routers and force both Active forwarders to be on the same router.
Router1 configs:
track 1 stub-object
interface *interface name*
ip address *ip address ip mask*
glbp *group number ip virtual ip address*
glbp *group number timers redirect interval value timeout value*
glbp *group number weighting track track number decrement decrement value*
Router2 configs:
interface *interface name*
ip address *ip address ip mask*
glbp *group number ip virtual ip address*
glbp *group number*
timers redirect interval value timeout value
Workaround: There is no workaround.

- CSCtf49950
Symptoms: Router that is configured with IPS experiences memory leak.
Conditions: This symptom occurs when IPS is configured.
Workaround: There is no workaround.
- CSCtf50867
Symptoms: Router reloads at iprouting_is_hdvrf_idb.
Conditions: This symptom occurs when configuring pri-group nfas_d with Cisco IOS Release 15.1(01.05)T.
Workaround: There is no workaround.
- CSCtf50992
Symptoms: MS Callback fails with local authentication.
Conditions: This issue is seen when we configure local authentication. There is no issue with RADIUS authentication.
Workaround: There is no workaround.
- CSCtf51156
Symptoms: On a Cisco router that is running ISIS with 1 second as hello interval, Compact flash removal and insertion may result in ISIS neighborship flap.
Conditions: This issue is observed when ISIS is configured with 1 second as hello interval.
Workaround: There is no workaround.
- CSCtf51690
Symptoms: Router will crash when a packet with out of bound featureIndex is sent to CME.
Conditions: This symptom occurs when malformed packets are being sent to CME with out of bound featureIndex values in fStationFeatureStatReqMessage.
Workaround: There is no workaround.
- CSCtf59960
Symptoms: DHCP pool does not assign IP add to other interface when virtual interface is configured and removed.
Conditions: This problem is seen in Cisco 7200 series router that is loaded with Cisco IOS Release 12.4(24)T3.
Workaround: There is no workaround.
- CSCtf62621
Symptoms: Cannot push the FW down to the VDSL chipset on the Cisco 887V modem.
Conditions: This symptom is observed on a Cisco 887V router with no startup-config in NVRAM.
Workaround: “wr me” and reload the router.

Resolved Caveats—Cisco IOS Release 15.1(1)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCef82896

Symptoms: When the user name in the authentication dialog box is left blank, the router unexpectedly reloads.

Conditions: The symptom is observed when authenticating via the HTTP server. It is observed only when a valid user name was previously configured:

```
(config)#ip http authentication local
(config)#username <name> privilege <number> password <password>
```

Workaround: Do not leave the user name blank in the authentication text box if username authentication is enabled.

- CSCsc49637

Symptoms: If a PPPoE client session is timed out (e.g. due to a network outage), and a restart of the session is subsequently unsuccessful (e.g. because network outage persists or the PPPoE server has not timed out the prior session) and if the user then manually clears the session, then the router will no longer be able to bring up this session until a reload is performed.

Conditions: This symptom has been observed when the PPPoE session is unexpectedly interrupted with Cisco IOS Release 12.3(8)T8 or Release 12.3(11) T5. The next feature also needs to be configured:

```
pppoe-client dial-pool-number 1 dial-on-demand
```

Workaround: Use the following procedure:

1. Reload.
2. Do not configure the DDR feature for the PPPoE session. This problem is limited to PPPoE client sessions using the DDR feature.

- CSCsc62963

Symptoms: The interface MTU is not user configurable. When you attempt to configure “interface level command mtu,” the following message is printed:

```
% Interface {Interface Name} does not support user settable mtu.
```

Conditions: The symptom is observed with a 2-Port FE on a Cisco 7200 series router.

Workaround: There is no workaround.

Further Problem Description: The Cisco.com document entitled *MPLS MTU Command Changes* further discusses this enhancement.

- CSCsh96558

Symptoms: A traceback may be generated during the “ipmcast_ipv6_rpf_lookup” function.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when you configure IPv6 multicast routing on both the PE router and a connected CE router, add an IPv6 address to the connected interfaces, and configure PIM sparse or PIM sparse-dense mode on both routers. The traceback is generated when the neighborship comes up after you have configured one of the interfaces as a PIM-RP.

Workaround: There is no workaround.

- CSCsl52962

Symptoms: The RP crashes due to a watchdog timeout of the uRPF stats process.

Conditions: The symptom is observed when issuing the **interface range port-channel number - number** command.

Workaround: There is no workaround.

- CSCsq71492

Symptoms: A Cisco IOS device may reload with an address error or have alignment errors and tracebacks such as

```
%ALIGN-3-SPURIOUS or %ALIGN-3-TRACE
```

Conditions: The symptoms are most likely to occur when the TACACS+ server (ACS) sends an “authentication error” when ACS is configured, or when a request timeout occurs. There may be other AAA- or TACACS-related conditions that cause the symptom.

Workaround: There is no workaround.

- CSCsr98707

Symptoms: When the main ATM interface MTU has an explicit non-default value (something other than 4470), then the subinterfaces may not save (shown with the **show run** command) the explicit MTU configuration of the default (4470) even though the command is expected.

Conditions: The symptoms are observed only for the ATM MTU value 4470. This unexpected behavior is not seen for any other value (less than or more than 4470 within allowed ATM MTU values).

Workaround: Upon reload, manually (explicitly) configure MTU 4470. You can configure an IP MTU under the ATM interface instead of an ATM MTU.

- CSCsu50869

Symptoms: Calls do not complete because Cisco Unified Border Element (CUBE) does not send PRACKs to all 1xx messages.

Conditions: This symptom is observed with h.323 slow start to SIP delayed media call flow.

Workaround: Enable fast start h.323 with an MTP in CUCM, which allows for SIP early offer. Reliable 1xx messaging can also be disabled to prevent the requirement of provisional acknowledgements.

- CSCsu78975

Symptoms: Crash seen @adj_switch_ipv4_generic_les on a Cisco 38xx router.

Conditions: This symptom is observed upon entering the command **no ip route 10.2.82.0 255.255.255.0 vlan1**.

Workaround: There is no workaround.

- CSCsv00168

Symptoms: Junk values are displayed on a Cisco router when characters or commands are entered. For example, when **show version** is entered, “h ^v^@e^@^r^@^@^@^@^@” is displayed.

Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

Workaround: There is no workaround.

Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv03300

Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

Conditions: This symptom is observed when a CBWFQ QoS policy is attached to the onboard gigabit ethernet interface.

Workaround: There is no workaround.

- CSCsv30540

Symptoms: The error message `%SYS-2-CHUNKBOUNDSIB` and a traceback are seen.

Conditions: These symptoms are observed when the **show running-config/write memory** command is entered.

Workaround: There is no workaround.

- CSCsw15188

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: This is seen when “logging host <address> session-id” is configured. Configuring “logging host <address>” without the additional keywords will not cause the problem.

This bug also requires certain log messages that use new lines, such as debugs from **debug isdn q931**.

Workaround: Disable the syslog server when doing the debugs.

- CSCsw18733

Symptoms: A Cisco 7200 router may crash while unconfiguring crypto ipsec tunnel with EzVPN client configurations.

Conditions: This symptom is observed when crypto ipsec tunnel is configured and then unconfigured.

Workaround: There is no workaround.

Further Problem Description: A Cisco 7200 router crashes when unconfiguring a virtual-template of the tunnel type.

- CSCsw52855

Symptoms: CRC and frame errors are seen if mark was used as the idle character between packets.

Conditions: This problem occurs when using the following interface cards:

- VWIC2-1MFT-T1/E1
- VWIC2-2MFT-T1/E1
- VWIC2-1MFT-G703
- VWIC2-2MFT-G703

Workaround: Use the following interface cards that are not affected by this problem:

- HWIC-4T1/E1
- HWIC-2CE1T1-PRI
- HWIC-1CE1T1-PRI

This is caveat has been closed.

- CSCsw62346
Symptoms: When unsupported filter is added to global policy-map with only match-any as the filter, the router or line card might crash.
Conditions: Occurs when global policy map is attached to an interface.
Workaround: Detach service policy from interface before making changes.
- CSCsw76113
Symptoms: Unable to reuse a sub-interface as main-interface.
Conditions: Occurs when we configure **no virtual-template subinterface** when all of the Interface Descriptor Blocks (IDB) that platform supports are used as “subif-vaccess”. No more “vaccess” can be created.
Workaround: Do not configure **no virtual-template subinterface** at run time. Check **show vtemplate** output. If there are more IDBs used by subinterface, then do not configure **no virtual-template subinterface**.
- CSCsx20147
Symptoms: The delay value to destination computed is different between IPv4 and IPv6.
Conditions: Occurs when EIGRP for IPv6 is configured.
Workaround: There is no workaround.
- CSCsx26025
Symptoms: Wireless clients are not able to ping each other after a few minutes.
Conditions: Can occur on any of the following routers with 802.11 wireless interfaces:
Cisco UC500, Cisco 85x, Cisco 87x, Cisco 1811, Cisco HWIC-AP
Workaround: There is no workaround.
- CSCsx32049
Symptoms: Traceback is observed and the system may reboot, depending on the platform.
Conditions: The symptom is observed when the ESM filter is configured and contains an ios_config statement.
Workaround: Remove ios_config statements from ESM filter.
- CSCsx75520
Symptoms: Ping is not working on a Cisco router with a ctunnel interface.
Conditions: This symptom is observed after attaching a policy map to a ctunnel interface.
Workaround: Delete the policy map from the ctunnel interface using the **no policy-map** command and reload the router.
- CSCsx75623
Symptoms: Tracebacks are seen when “create on-demand” is configured on a VC class and when an OIR is performed on the ATM interface.
Conditions: This symptom occurs only if an OIR is performed when the configurations are made.
Workaround: There is no workaround.
- CSCsx93245
Symptoms: A Cisco router may reload after issuing the **show gatekeeper zone prefix all** command.
Conditions: This symptom is observed on a Cisco 3825 router running Cisco IOS Release 12.4(8a).

Workaround: There is no workaround.

- CSCsy10893

Symptoms: A Cisco router reloads occasionally after the command **show buffers leak** is repeatedly entered.

Conditions: The symptom is observed when entering the **show buffers leak** command. It occurs only with certain patterns and scale of traffic and does not occur all the time.

Workaround: There is no workaround.

- CSCsy19751

Symptoms: Several chunk element leakages are seen when the **show memory debug leaks chunk** command is entered.

Conditions: Occurs after a reboot.

Workaround: There is no workaround. Please ignore the leaks as they are false alarms.

- CSCsy34256

Symptoms: Tracebacks are observed when the trustpoint is removed abnormally and the **no sccp** and **sccp** commands are entered.

Conditions: This symptom is observed when the **no sccp** and **sccp** commands are entered after the trustpoint has been removed abnormally.

Workaround: There is no workaround.

- CSCsy41063

Symptoms: A Cisco router may display the following error message:

```
%SYS-2-BADBUFFER: Attempt to use Mismatch sized buffer as scattered src, ptr=
83BB71E0, pool= 83A4F670 -Process= "<interrupt level>", ipl= 2, -Traceback= 0x808DA290
0x80087808 0x801BAF9C 0x800E5954 0x800E73F0 0x80369148 0x8008590C 0x8008590C
0x80369208 0x8036D334 0x81957024 0x8036B57C 0x80375294
```

Conditions: This symptom is observed with Q-in-Q configuration on the device.

Workaround: There is no workaround.

- CSCsy49927

Symptoms: IOSD restart seen with crest proc that fetches the tcl shell for execution.

Conditions: This symptom is observed with a crest proc that helps in configuring a scale configuration.

Workaround: There is no workaround.

- CSCsy54137

Symptoms: Some calls are shown as active after a WAN link outage between the gateway and Call Manager.

Conditions: The symptom is observed if a WAN outage happens when more than 40 calls are in progress. Some random calls are then shown to be as active when using the command **show call active voice compact** with Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCsy61321

Symptoms: Accounting requests sent to the TAC server do not fail over to the second server.

Conditions: This symptom is observed when two TACACS servers are configured, the first without TACACS, the second with TACACS, and authentication is configured as "none."

Workaround: Use a single working server, or ensure that the first group uses a valid server.

- CSCsy70524

Symptoms: A router crashes upon deleting range PVCs with PPPoE sessions and with bandwidth configured through DBS.

Conditions: The symptom is observed when deleting the range PVCs with PPPoE sessions.

Workaround: There is no workaround.

- CSCsy74023

Symptoms: A slow memory leak occurs, mainly in the 72 bytes, 80 bytes, and possibly 192 bytes memory regions blocks.

Conditions: This symptom is observed with a large number of IPsec peers (>100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

Workaround: There is no workaround.

- CSCsy89795

Symptoms: A Cisco ASR 1000 series router may fail, and the console will display an error message similar to the following:

```
"A critical process ppc_linux_iosd_image has failed (rc 139)".
```

Conditions: This symptom is observed when using the **clear counters** command after removing a crypto map from an interface.

Workaround: Wait a minute or two after removing a crypto map from an interface before entering the **clear counters** command.

- CSCsz18573

Symptoms: A number of problems are found in the early version of the NEMO mobile router:

- MR tunnel will flap with NEMO explicit prefix configured.
- Roaming can be slow or fail installing routes.
- MR routes appear as static as opposed to mobile.
- Configuring the home address on a loopback is required.
- ND operates on the MIP tunnel.
- Ten seconds latency appears on MR at tunnel setup and on HA at roaming.

Conditions: These symptoms occur when running Cisco IOS Release 12.4(22)T1 and Release 15.0(1)M.

Workaround: There is no workaround.

- CSCsz29542

Symptoms: In the current implementation, "cwmmp agent" identifies the WAN uplink if it has "cwmmp wan default" configured on it. The WAN uplink interface differs, based on the router type used as a CPE. For the Cisco 871 router, WAN interface is FastEthernet 4 and for a Cisco 2811 router it is Fast Ethernet 0/0. This creates a problem in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

Conditions: The symptom is observed in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

Workaround: There is no workaround.

- CSCsz39167

Symptoms: If a tunnel is configured over the 880-3G cellular interface, traffic forwarding stops when the packet size is greater than the tunnel MTU.

Conditions: The symptom is observed when a tunnel is configured over a cellular interface and running Cisco IOS Release 12.4(24)T.

Workaround: Disable “ip cef.”

- CSCsz68709

Symptoms: A console may lock when using the **scripting tcl init** *init-url* command.

Conditions: This symptom is observed when using the **scripting tcl init** *init-url* command where the *init-url* is invalid or inaccessible, then entering the **tclsh** command and appending a file name.

Workaround: Ensure that the *init-url* argument used in the **scripting tcl init** command is valid and accessible.

Alternate workaround: Enter the **tclquit** command to end the Tcl shell and return to privileged EXEC mode, then enter the **tclsh** command to enable the Tcl shell again.

- CSCsz71787

Symptoms: A router crashes when it is configured with DLSw.

Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

Cisco IOS devices that are configured for DLSw with the **dls w local- peer** command automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dls w local-peer peer-id IP- address** command listens for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dls w remote-peer 0 fst <ip-address>
```

It is possible to disable UDP processing in DLSw with the **dls w udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dls w remote-peer 0 fst <ip-address>
```

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature.
access-list 111 deny udp host 192.168.100.1 any eq 2067 access-list 111 deny 91 host
192.168.100.1 any
!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.
access-list 111 permit udp any any eq 2067 access-list 111 permit 91 any any
!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.
class-map match-all drop-DLSw-class match access-group 111
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-DLSw-traffic class drop-DLSw-class drop
!--- Apply the Policy-Map to the Control-Plane of the
!--- device.
control-plane service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic class drop-DLSw-class police 32000 1500 1500
conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dls w udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
!--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067 access-list 150
deny 91 any INFRASTRUCTURE_ADDRESSES MASK
!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations.
!--- Permit all other traffic to transit the device.
access-list 150 permit ip any any
interface serial 2/0 ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in a customer environment.

- CSCsz72142

Symptoms: Memory corruption may occur.

Conditions: This symptom may be observed after issuing the **clear ip bgp soft** command on a BGP session which includes a connector attribute.

Workaround: There is no workaround.

Further Problem Description: This symptom was found by automated analysis tools, but has not been seen to have any real-world impact.

- CSCsz83570

Symptoms: SSH sessions disconnect during large data exchanges, such as large logs with pagers.

Conditions: The symptom is observed when large amounts of data are exchanged between both ends: client and server (i.e.: the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

Workaround: Use 3DES for encryption.

- CSCsz89093

Symptoms: A Cisco 2800 router may drop multicast packets.

Conditions: This symptom is observed when stream sources are connected to an NM-16ESW switch module.

Workaround: Disable IGMP snooping.

Further Problem Description: Packet loss can be seen with as little as 1 stream consisting of 1500 byte packets @ >= 1470pps. Packet loss can be viewed as follows:

```
zmr# zmr#sh int Fa1/1 stat
FastEthernet1/1 Switching path Pkts In Chars In Pkts Out Chars Out Processor 100000
150000000 53 4028 Route cache 0 0 0 0 Total 100000 150000000 53 4028 <--- 100,000 pkts
received zmr# zmr#sh int Vlan200 stat
Vlan200 Switching path Pkts In Chars In Pkts Out Chars Out Processor 0 0 0 0 Route
cache 99997 149595512 0 0 Total 99997 149595512 0 0 <--- 3 pkts dropped zmr#
```

- CSCsz89826

Symptoms: The router starts reloading while testing the OAM management functionality over ATM using the encapsulation aal5mux ppp which is done after the encapsulation aal5snap.

Conditions: This symptom is observed after configuring “oam-pvc manage 9” under OAM feature.

Workaround: There is no workaround.

- CSCsz93306

Symptoms: Cisco IOS SCEP replies with the configured hash and encryption algorithm (the default is md5/des), instead of replying with the hash and encryption algorithms used by the client.

Conditions: This symptom is observed under normal conditions.

Workaround: Since the main concern is that less secure algorithms may be used in the reply than the request, administrators can match the algorithms configured for the clients in the Cisco IOS CA.

That being said, you can only set the hash algorithm, and not the encryption algorithm. For that there is no workaround.

- CSCta08194

Symptoms: A router may crash.

Conditions: This symptom is observed when reprovisioning an AToM tunnel with AAL5 encapsulation.

Workaround: There is no workaround.

Further Problem Description: A complex sequence of events with specific timing characteristics is required to hit this crash.

- CSCta09049

Symptoms: A memory leak chunk in alloc-proc “encrypt proc” with the name “Packet Header” is observed.

Condition: This symptom is observed with software crypto enabled. The same configuration and traffic running with onboard-VPN does not have the leak.

Workaround: Configure “no ip cef optimize neighbor resolution.”

- CSCta11223

Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

Workaround: There is no known workaround.

- CSCta14505

Symptoms: No source group (SG) entry forms in the network for PIM sparse-mode groups. This leads to traffic failures.

Conditions: This symptom is observed when PIM-SM is configured in the network and traffic is sent for PIM-SM groups.

Workaround: Shut down the upstream interface, remove the IP address, configure it again, then perform a **no shutdown** on the interface.

- CSCta16724

Symptoms: Users with level 15 privilege and a “view” cannot do a Secure Copy (SCP).

Conditions: The symptom is observed when a user with a “view” attempts to do an SCP.

Workaround: Remove view.

- CSCta17774

Symptoms: An abnormal/high interarrival jitter time is reported in RTCP from a Cisco AS54xx when Nextport DSPs are used.

Conditions: This symptom is observed under the following conditions:

- Nextport DSPs are used on a Cisco AS54xx.
- RTCP is used to measure interarrival jitter values.

Workaround: There is no workaround.

- CSCta19962

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml>.

- CSCta20590

Symptoms: A group member (GM) pseudotime may desynchronize after re- registering or at initial registration.

Conditions: This symptom is observed when GETVPN with time-based anti-replay (TBAR) is enabled.

Workaround: Disable TBAR or use a very large window (> 30 seconds).

Further Problem Description: After establishing phase I, the GM is supposed to obtain the KEK and TEKs. If a packet drop occurs (usually, this message is fragmented across multiple frames), then the router is not able to reassemble the packet. IKE will later resend this message, but if the pseudotime has not been recalculated the symptom will reoccur.

- CSCta21492

Symptoms: PPP callback may fail.

Conditions: This symptom is observed when MLP is configured under the dialer.

Workaround: There is no workaround.

- CSCta22767

Symptoms: A Cisco router may crash when unconfiguring class-map.

Condition: This symptom is observed in a Cisco router using Cisco IOS Release 15.0M.

Workaround: There is no workaround.

- CSCta30439

Symptoms: Cisco routers with NPE-G1 and NPE-G2 may crash.

Conditions: This symptom is observed when MLP is configured on CJ-PA and OIR is performed.

Workaround: There is no workaround.

- CSCta32825

Symptoms: A Cisco router may crash with a bus error after configuring a class-map or modifying a class-map.

Conditions: This symptom is observed when using the **class-map** command in global configuration mode and the **match** command in class-map configuration mode. For example, entering the following commands may result in a crash:

```
*router(config)#class-map match-any PRIO
*router(config-cmap)#match dscp cs4
*router(config-cmap)#match dscp cs4 af41
*router(config-cmap)#match dscp cs4 af41 af42
*router(config-cmap)#match dscp cs4 af41 af42 af43
*router(config-cmap)#match dscp cs4 af41 af42 af43 ef
*router(config-cmap)#match dscp cs4 af41 af42 af43 ef cs5 <---device crashes here
```

Workaround: Configure QoS changes when no traffic is passing through the router. This has only been seen while traffic is trying to match against the policy while it is being updated.

- CSCta37063

Symptoms: NAT fails to translate H323 payload information.

Conditions: This symptom occurs when NetMeeting is dialing from outside NAT to inside NAT.

Workaround: Initiate NetMeeting again. Note that once this NAT entry is cleared or has timed-out, the issue will reappear.

- CSCta39339

Symptoms: Traffic loss occurs on a Cisco ES20 line card when configuring IPv4 IP address on the SVI interface.

Conditions: This symptom is observed when an xconnect configuration exists.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the SVI interface.

- CSCta49840

Symptoms: GGSN may encounter a fatal error in VPDN/L2TP configurations.

Conditions: The symptom is observed in rare race conditions when physical connectivity on the interface to LNS is lost while there are active sessions and traffic.

Workaround: There is no workaround.

- CSCta50110

Symptoms: A GM does not register.

Conditions: This symptom is observed when a crypto map is attached to a tunnel interface only.

Workaround: Apply the crypto map to the tunnel source physical interface as well.

- CSCta56762

Symptoms: A Cisco router acting as an IP SLA Responder may leak memory in the chunk manager.

Conditions: The symptom is seen when the router is responding to VoIP RTP probes.

Workaround: Stop the probes.

- CSCta59045

Symptoms: If 32k dual-stack sessions are configured on a PTA device such as a Cisco ASR 1000, the router may crash when the sessions are brought down.

Conditions: This symptom is observed when both the PPPoE client and the PTA are Cisco ASR 1000 routers. The client crashes when the **test pppoe** command is entered while trying to bring up 16K dual-stack sessions on the PTA device. This symptom is more likely to be observed when the preferred lifetime and valid lifetime of the assigned prefix are configured to be equal. The crash may occur even if the lifetimes are not equal, but it is less likely.

Workaround: Do not configure the valid and preferred lifetimes of the prefix equally. This will decrease the probability of this crash, but does not ensure against it.

- CSCta66499

Symptoms: The Cisco IOS MGCP gateway may experience a software-forced reload.

Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T4 or a later release when reenabling MGCP with version 1.0 after testing fgds calls with MGCP version 0.1.

Workaround: There is no workaround.

- CSCta69213

Symptoms: A Cisco router configured for NHRP may crash due to a bus error.

Conditions: This symptom is observed on a Cisco router configured for NHRP and DMVPN.

Workaround: There is no workaround.

- CSCta75923

Symptoms: One-way voice may occur after a transfer through a CMM transcoder if the stream goes through an RTP-aware firewall such as an ASA. The transcoder in some transfer situations will reuse a previous SSRC, which causes a security violation.

Conditions: In a situation where there are 3 SSRCs in a single transfer, the outgoing stream from the transcoder will reuse the first SSRC in place of the third SSRC. This is against the RTP RFC, and some firewalls may drop the packet. Some gateways and endpoints may also not correctly process the packets, depending on the strictness of the RFC implemented.

Workaround: It was found that some endpoints, like the Cisco Unified IP Phone 7960, activated a transfer with only 2 SSRC changes. It was also found that a Cisco Unified IP Phone 7941 with firmware 8-3-2 had the problem, but the latest 8-4-X image did not. Some endpoints, such as an autoattendant, do not have the ability to change this behavior. The only other workaround is to use a different type of transcoder than the ACT CMM.

- CSCta76251

Symptoms: VPLS AD may not work after BGP has converged.

Conditions: This symptom is observed when all of the PE routers are reloaded at the same time.

Workaround: Configure MPLS IP by entering the **mpls ip** command on one of the tunnel interfaces.

- CSCta77678

Symptoms: RTP timestamp on the RFC 2833 event is modified. IP Phones are using RFC2833 to transport the DTMF signals, which causes problems with the Voicemail systems.

Conditions: This symptom occurs when RTP header compression is enabled.

Workaround: There is no workaround.

Further Problem Description: The problem disappears if cRTP is disabled. The issue is seen with Class-Based cRTP configured and also with other cRTP configuration types.

- CSCta77960

Symptoms: TCP/TCB leak may occur on a Cisco voice gateway with an increasing number of sessions hung in CLOSEWAIT state.

Conditions: This symptom occurs when the voice gateway is under normal use.

Workaround: There is no workaround.

- CSCta92029

Symptoms: MSDP SA is not received on an MSDP peer.

Conditions: The symptom is observed when the first hop router is also the RP.

Workaround: There is no workaround.

- CSCta93129

Symptoms: An IP fragment may bypass virtual fragment reassembly (VFR) processing and create a VFR timeout, causing additional inner IP fragments to be dropped.

Conditions: This symptom is observed when encrypted IPSEC packets are fragmented by the remote device (fragmentation after encryption) or somewhere in the network between the VPN termination routers. When the fragmented IPSEC packets are reassembled and decrypted, if the decrypted inner packet is also an IP fragment, the IP fragment bypasses VFR processing. The following conditions may cause this symptom to occur:

1. VFR is enabled on the decryption side
2. Fragmentation happens after encryption on the encrypting router, or in the path
3. The inner IP packet is fragmented when received by the encrypting router.

Workaround: Perform fragmentation before encryption on the sending side, and ensure that the proper IP MTU is used on the tunnel so that no fragmentation occurs after encryption.

Further Problem Description: When IPSEC packets corresponding to the first inner IP fragment bypass VFP processing, the second inner IP fragment, even if too small to require IPSEC fragmentation, is decrypted and then sent for VFR processing. Due to the timeout created when the first IP fragment bypasses VFR processing, the second inner IP fragment is dropped.

- CSCta93703

Symptoms: Packets may be sent out of order in an rfc4938 flow-controlled PPPoE session.

Conditions: This symptom is observed when packets are queued due to insufficient credits and a traffic stream is active.

Workaround: There is no workaround.

- CSCta94296

Symptoms: Some voice commands go missing, the router freezes on bootup, or there may be a crash on bootup with the following message:

```
%ALIGN-1-FATAL: Illegal access to a low address.
```

This is possibly seen with “Unable to save the data for mode. Too many saves” being printed on bootup.

Conditions: The symptom is observed when many global voice or CME commands are configured.

Workaround: Remove some global voice or CME feature commands.

- CSCta95295
Symptoms: A Cisco router terminates 100+ VPN tunnels when using CRL checking for the Phase 1 authentication.
Conditions: If IKE gets stuck for any reason, it might cause IOMEM to be depleted completely, which could lead to a router crash.
Workaround: Disable CRL checking or use pre-shared keys.
- CSCta95621
Symptoms: Firewall performance degradation is seen for HTTP traffic.
Conditions: The symptom is observed when configuring a Zone Based Firewall to match HTTP traffic.
Workaround: There is no workaround.
- CSCta96479
Symptoms: IPv6 PPPoX session setup rate is low, dropping to about 10 sessions per second.
Conditions: This symptom is observed under the following conditions:
 1. High number of PPPOX sessions with ipv6 ACLs
 2. IPV6 ACEs use port number
 3. IPV6 ACEs use icmp fields
 Workaround: There is no workaround.
- CSCta98321
Symptoms: AAA server for HTTP authentication cannot be configured on a Cisco 861 integrated services router (ISR).
Conditions: This symptom is observed when configuring the AAA server for HTTP authentication on a Cisco 861 ISR.
Workaround: There is no workaround.
- CSCta98976
Symptoms: A Cisco IOS certificate server (CS) may crash during a CA certificate rollover.
Conditions: This symptom is observed with similarly-named keys.
Workaround: Rename similarly-named keys. For example, the keys named SubCA are a subset of the SSH keys named SubCA.server. Rename the SSH keys using the **ip ssh rsa keypair-name** command.
- CSCtb01505
Symptoms: A Cisco router may crash when building an OSPF Network LSA.
Conditions: This symptom is observed while unconfiguring ospf configurations.
Workaround: There is no workaround.
- CSCtb05195
Symptoms: Throughput degradation may occur on a Cisco integrated services router (ISR).
Conditions: This symptom is observed in CEF/SVI TOE configurations when comparing specific performance metrics between baseline Cisco IOS Release 12.4 (23.5)pi10 and target Release 12.4(24.6)PI11n.
Workaround: There is no workaround.

- CSCtb09167

Symptoms: The following issues can be observed with the PI11 image with a simple setup on both NPE-G1 and NPE-G2:

1. There is a ~50% degradation on forwarding performance (with service reflect) on NPE-G1 when compared with Cisco IOS Release 12.4T.
2. When the traffic rate goes higher than the router's capacity, traffic will not recover afterwards, even if the traffic is reduced back to a very low rate.

Conditions: The symptom is specific to the service reflect feature.

Workaround: There is no workaround.

- CSCtb11373

Symptoms: Enabling IPv6 inspection debugs may lead to a Cisco router crash when traffic is passing through the device.

Conditions: This symptom is observed in Cisco IOS Release 12.4(21) with the following debug commands:

- **debug ipv6 inspect tcp**
- **debug ipv6 inspect detailed**
- **debug ipv6 inspect events**

Workaround: Do not use the above IPv6 inspection debug commands.

- CSCtb13015

Symptoms: Virtual access on the LNS fails to obtain the template IP address.

Conditions: This symptom is observed when

1. a VPN profile template cisco-avpair is configured as follows:

```
template:ip-addr=10.10.10.10 255.255.255.255
```

2. A PPPoE session is established from the client to the LNS. The call comes up, but the virtual access on the LNS fails to obtain the template IP address "10.10.10.10."

Workaround: There is no workaround.

- CSCtb13421

Symptoms: The GM may not register on a Cisco ASR 1000 series router.

Conditions: This symptom is observed when a crypto map with local-address configured is applied on multiple interfaces, and one of these interfaces is then shut.

Workaround: Disable local-address for the crypto map.

- CSCtb13472

Symptoms: An LDP session flap occurs between PE and P routers. A large number of LDP sessions going down may cause all LDP sessions within the routing context to go down temporarily, and then come back up (i.e.: flap).

Conditions: This symptom is observed with 100 LDP-targeted sessions between the PEs. When the targeted sessions flap, the link session between PE and P routers also flaps. The symptom is not restricted to just targeted sessions flapping. Any large number of LDP sessions flapping within a routing context could cause all LDP sessions within the routing context to flap. In this example, all the LDP sessions are within the default (non-VRF) routing context.

Workaround: There is no workaround.

- CSCtb17152
Symptoms: A large packet drop may occur when FRF.12 is enabled.
Conditions: This symptom is observed when FRF.12 is enabled.
Workaround: There is no workaround.
- CSCtb17856
Symptoms: H323 calls may intermittently fail with Cause Code 41. After several days and depending on traffic, calls may start failing with Cause Code 47.
Conditions: This symptom is observed when there is a race condition in setting up an H245 session between H323 peers and two separate H245 sessions are opened simultaneously.
Workaround: There is no workaround for Cause Code 41. For Cause Code 47, reload the router to temporarily alleviate the symptoms.
- CSCtb21428
Symptoms: An interface does not attempt to restart after restart-delay is configured.
Conditions: When the serial interface is down for some reason and you have configured restart-delay on the serial interface, the interface should try to restart.
Workaround: There is no workaround.
- CSCtb22889
Symptoms: SIP(TLS--SIP CUBE) may experience up to 2-3 seconds of post-dial delay due to TLS processing. Processing delays of 1000 ms, 600ms, and 200ms are seen between the gateway TLS responses.
Conditions: This symptom is observed with a TLS connection to another gateway.
Workaround: Use the **sip-ua timers connection aging tls time** command to increase the time in the gateway TLS aging timer and therefore lower the frequency of the problem with the aging TLS timer.
- CSCtb25549
Symptoms: Router crashes.
Conditions: The symptom is observed with the following sequence:
 1. Use the command **debug condition username**
 2. Bring up a VPDN session
 3. Clear the VPDN tunnel on LAC
 4. Remove the conditional debug.
 Workaround: There is no workaround.
- CSCtb26396
Symptoms: HTTPS connections suddenly fail with the following error:


```
//-1//HTTPC:/httpc_ssl_connect: EXIT err = -3, hs_try_count=1
//394376//HTTPC:/httpc_process_ssl_connect_retry_timeout: SSL socket_connect failed
fd(0)
```

 Conditions: The symptom is observed with CVP Standalone deployment running with HTTPS and with Cisco IOS Release 12.4(22)T1 or Release 12.4(24)T1.
Workaround: Reload the gateway.

- CSCtb27747

Symptoms: An active RP module may crash or the entire system may reload while the user is scrolling through the output of the **sh xconnect rib detail** command.

Conditions: This symptom is observed when remote PEs in the VPLS mesh are reloading and some are in the process of booting up. The user has to pause and then continue the output of the **sh xconnect rib detail** command while the remote PEs are being added or deleted.

Workaround: Do not enter the **sh xconnect rib detail** command while remote PEs are being added or deleted.

- CSCtb34358

Symptoms: Tunnel sources get mixed up when tunnel interfaces are configured with serial subinterfaces as sources and the router is reloaded.

Conditions: The symptom occurs only after a reload or when a saved configuration is applied to the running configuration.

Workaround: There is no workaround.

- CSCtb34814

Symptoms: The following error message is reported just before a crash:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

There may not be any tracebacks given for the crash.

Conditions: This symptom is observed under normal conditions.

Workaround: There is no workaround.

- CSCtb36521

Symptoms: A Cisco Catalyst 6500 may stop processing IKE traffic, which results in IPSec tunnels not working. Under extreme circumstances, system IO memory might become completely depleted, at which point all traffic processing will stop.

Conditions: This symptom is observed on a Cisco Catalyst 6500 with a VPN-SPA module running a Cisco IOS SXH image when PKI infrastructure is used to authenticate IKE peers. The certificate in use must contain a CDP that uses HTTP protocol to retrieve the CRL. Revocation-check must be configured to fetch the CRL using the **revocation-check crl** or **revocation-check crl none** command.

Workaround: Disable CRL validation by using the **revocation-check none** command instead of the **revocation-check crl** or **revocation-check crl none** commands in the trustpoint being used. Note that disabling CRL validation poses a possible security risk.

Alternate Workaround: Create a certificate map tied to the trustpoint in use to override the CDP using a URL which specifies the IP address of the CDP server instead of a name. For example, if the router1 certificate tied to cdp_override trustpoint contains a CDP URL such as:

```
http://ca_server.yourdomain.com:80/crl.txt
```

replace it with the ca_server.yourdomain.com IP address by using:

```
crypto pki trustpoint cdp_override match certificate cert_map_1 override cdp url
http://XXX.xxx.x.x:xx/crl.txt
```

```
crypto pki certificate map cert_map_1 1 subject-name co router1
```

- CSCtb36637

Symptoms: The registering flag gets set on Mroute entry. Register-Stop is not received from the RP.

Conditions: The symptom is observed when sending the data packets before the RP address interface comes up in RP. It is observed on a Cisco 7200 series router that is running the 12.4(24.6)PI11r image.

Workaround: There is no workaround.

- CSCtb37756

Symptoms: A Cisco router acting as NAS rejects an IPCP request from the client.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24.6) under the following conditions:

1. Clients connect over BRI lines and legacy dialer is configured on both the clients and NAS
2. Multilink is configured on the client and NAS [Dialer Hunt group scenarios]
3. Radius authentication is used and, during authentication, per-user attributes are downloaded.

Workaround: Configure the RADIUS server so that per-user attributes are not sent in Access-Accept or Access-Challenges (EAP case). Since this is Legacy Dialer and BRI, multiple user sessions are not really seen and hence the required attributes can be configured locally on router.

- CSCtb39345

Symptoms: Session timeout does not occur within the time configured in the session-timeout value on a per-user profile.

Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M.

Workaround: There is no workaround.

- CSCtb40985

Symptoms: The memory occupied by the Cisco IP SLAs Sync Pro may gradually increase.

Conditions: This symptom is observed on a Cisco Supervisor Engine 720 (sup720- 3B) with a Cisco IOS Release 12.2(33)SX11 image when ICMP path jitter operation is configured on the router with an invalid source address.

Workaround: Configure the SLA operation with the correct source address.

- CSCtb43009

Symptoms: A Cisco 3845 router crashes when key server is removed from the list.

Conditions: The symptom is observed with the following configuration on a GM router:

```
conf t crypto gdoi group GetvpnScale1 identity number 1111 no server address ipv4
10.10.1.4
```

When a unicast rekey is received, the router crashes.

Workaround: There is no workaround.

- CSCtb43293

Symptoms: ACL functionality may break on a Cisco 10000 series router after redundancy switchover.

Conditions: This symptom is observed after a redundancy switchover on a PPPoX session with ACL applied.

Workaround: There is no workaround.

- CSCtb44031

Symptoms: An LDP session goes down and does not re-establish.

Conditions: This symptom is observed when the password is removed from the LDP session on both peers with the **no mpls neigh ip- address password password** command.

Workaround: There is no workaround.

- CSCtb44167

Symptoms: A Cisco router may reload when running EAP- FAST authentication with RADIUS Accounting.

Conditions: This symptom is observed on a Cisco 1841 integrated services router that is running Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCtb45057

Symptoms: A fax through a Cisco IOS gateway configured for Fax Relay to a Cisco fax server fails.

Conditions: When there is an incoming fax call on the Cisco IOS gateway that is configured for Fax Relay, the fax call setup between the gateway and the Cisco fax server fails. This symptom occurs when the Cisco fax server is configured to receive calls on an H.323 call control module.

Workaround: There is no workaround. Configure SIP between the Cisco IOS gateway and the Cisco fax server if that is an acceptable workaround.

- CSCtb45718

Symptoms: A Cisco router may crash with traceback leading to checkheap.

Conditions: This symptom is observed when endpoint agnostic port allocation has been enabled using the **ip nat service enable-sym-port** command.

Workaround: Disable the endpoint agnostic port allocation using the **no ip nat service enable-sym-port** command.

Further Problem Description: Under certain conditions, the symmetric port database is not in sync with the port list, resulting in the reuse of port ranges that had been free.

- CSCtb46556

Symptoms: With a CIPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2, the NPE-G2 sometimes crashes when executing the command **clear int range multilink 1 10** and the NPE-G1 gives spurious access for the same command.

Conditions: The symptoms are observed with a CIPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2 and when 14 multilinks are configured with two members each. Pagents are sending bi-directional traffic.

Workaround: Do not perform commands across all interfaces using interface range. Perform the commands one-by-one, manually.

- CSCtb48397

Symptoms: A Cisco ISR router may experience performance degradation due to corrupted TCP headers.

Conditions: This symptom is observed on a Cisco ISR router with Cisco IOS Release 12.4 or Release 12.4T running interface-based TCP header compression on any data link. Corrupted TCP headers may occur when all of the following are true:

1. Frame-Relay, PPP, or HDLC is configured with "ip tcp header-compression"
2. The queueing mechanism is fair-queue (either interface-based or in map- class frame-relay)
3. >1 TCP sessions are traversing the compressing mechanism
4. The packets are in the hardware (CEF) switching path.

Workarounds:

1. Do not configure an interface to carry compressed TCP/IP headers using the **frame-relay ip tcp header-compression** command.
2. Disable hardware switching for all interfaces on the Cisco ISR using the **no ip route-cache** command.
3. Do not use any form of fair-queue on interfaces configured with the **frame-relay ip tcp header-compression** command. To remove fair-queue, use the **no fair-queue** command in policy-map class configuration mode.

Further Problem Description: With exactly two MS Remote Desktop Protocol TCP sessions, when the UUT's serial transmit-ring (or frame-relay shaper Bc) congests and the fair-queue invokes, the compressed header from the second- established TCP flow is erroneously written into headers of some packets from the first-established TCP flow, resulting in post-decompression frames erroneously added to the first-established TCP flow and erroneously removed from the second-established TCP flow, thereby causing a performance degradation.

- CSCtb48984

Symptoms: SSLVPN Login Page is not being properly displayed on mobile devices. Also, there is no support for iPhone and iPod safari browsers.

Conditions: The symptom is observed on an access page using Windows Mobile, or on an iPhone or iPod.

Workaround: Page will be displayed but quality will be poor.

- CSCtb51922

Symptoms: Chunk leak of list element when a host-address under a PfR API provider is configured or unconfigured.

Conditions: This symptom is observed when the following occur:

1. PfR MC is configured
2. API provider with a host address is configured
3. Host address is unconfigured, or the MC process is shut/no shut.

Workaround: There is no workaround.

- CSCtb51993

Symptoms: A router crashes upon bringing up PPPoE sessions.

Conditions: The symptom is observed when AAA proposes a pool name but the pool is not defined on the NAS as well as the radius.

Workaround: Define the pool on the NAS or as a dynamic pool on the radius.

- CSCtb52200

Symptoms: A router may crash when configuring 3-level policies with strict priorities on each level.

Conditions: This symptom is observed when:

- the bandwidth value configured for the interface is very low
- a class in the parent policy has a bandwidth of less than 1kbps
- a child policy is added with priority or Bandwidth Remaining Percentage (BRP).

Workaround: When attaching a child policy with priority or BRP, ensure that the parent class bandwidth is greater than 1kbps.

- CSCtb54422

Symptoms: An MFR bundle moves from SW to HW mode and flaps after reload.

Conditions: This symptom is observed on a Cisco 7200 router when an MFR is configured on CJ-PA, then one member is added from MCTE1 and the following commands are entered: **wr mem** and **reload**.

Workaround: Create a new MFR after reload and add members to it.

- CSCtb56567

Symptoms: A Cisco voice gateway experiences a memory leak error on CCSIP SPI CONTROL process, which may lead the router to crash every 4-5 days.

Conditions: This symptom is observed when a router is configured with sip-ua using the **mwi-server** command with transport set to *tcp*, but the server specified is not set up to receive sip and thus replies with tcp resets. This can be caused by misconfigured sip mwi.

Workaround: Reload the device regularly to free the memory.

- CSCtb57180

Symptoms: A router may crash with a software-forced crash.

Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x>
Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.
3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.
4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.
5. Avoid issuing the **show users** command repetitively in a short period of time.

Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- CSCtb57237

Symptoms: After a call is resumed from hold, the gateway sends a G.729 codec although a G.711 was negotiated in the H.245 messages.

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T1.

Workaround: There is no workaround.

- CSCtb58160

Symptoms: A router crashes upon bootup.

Conditions: The symptom is observed when reloading a router with the NAM module configured.

Workaround: There is no workaround.

- CSCtb58724

Symptoms: The symptoms are:

1. Incomplete rekey/ANN seqnum checking. This may cause inaccuracy in detecting seqnum errors in Co-operative key server (COOP KS) split/merge corner cases.
2. After using the command **clear cry gdoi** on the GM, the GM may not register successfully due to a PST difference between the key server and the GM.

Conditions: The symptom is observed in corner cases of COOP KS split/merge scenarios.

Workaround: There is no workaround.

- CSCtb60603

Symptoms: The router crashes and resets when you try to execute the following command: **show run | format x** (where x = any keyword).

Conditions: The symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(24)T. The router needs to have a general route-map configured.

Workaround: Do not execute **show run | format x** if there is a general route-map configured in the router.

- CSCtb62177

Symptoms: Downspeeding stops based on Voice and 4-second silence.

Conditions: This symptom is observed on a Cisco AS5400.

Workaround: An image with a partial short-term solution was released on 08-09-2009. With this image, module changes are done, and the CLI is implemented to drop 4-second silence events and voice packets.

- CSCtb64686

Symptoms: When a VC bundle is configured and traffic is passed at a high rate, the output packet counters may show an incorrect and very large value.

Conditions: This symptom is observed only in Frame Relay PVC counters. The **show interface** command displays proper output.

Workaround: There is no workaround.

- CSCtb65151

Symptoms: A device might crash with a bus error and the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

Conditions: The symptom is observed on a device that is running Cisco IOS Release 12.4(24)T1. Other releases may be affected (those running with the Common Classification Engine). The condition seems to be temporary and after a while it goes away.

Workaround: There is no workaround.

- CSCtb66295

Symptoms: No ip connectivity exists due to erroneous ARP tables.

Conditions: This symptom is observed when NAT and HSRP are configured on the same interface.

Workaround: There is no workaround.

- CSCtb66925

Symptoms: A router may crash during a port scan to TCP port 53.

Conditions: DNS functionality must be configured on the device.

This crash has been observed only in Cisco IOS Release 12.4(24)T, Release 12.4(24)T1, and Release 12.4(22)T. It is a timing condition on processing DNS TCP traffic.

Workaround: Create an ACL to deny traffic to the device on TCP port 53:

The following mitigations have been identified for this Cisco bug ID, which may help protect an infrastructure until an upgrade to a fixed version of Cisco IOS software can be scheduled:

* Infrastructure Access Control Lists (iACLs)

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access list, which will protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: DNS over TCP
!---
access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
      INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
!---
!--- Deny DNS TCP traffic from all other sources destined
!--- to infrastructure addresses.
!---
access-list 150 deny tcp any
      INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
```

```

!---
access-list 150 permit ip any any
!---
!--- Apply access list to all interfaces (only one example
!--- shown).
!---
interface serial 2/0
ip access-group 150 in

```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Receive ACLs (rACLs)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the Cisco 12000, 12.0(24)S for the Cisco 7500, and 12.0(31)S for the Cisco 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor.

Receive ACLs are designed to protect only the device on which they are configured. On the Cisco 12000, 7500, and 10720, transit traffic is never affected by a Receive ACL. Because of this, the destination IP address “any” used in the example ACL entries below refer only to the router’s own physical or virtual IP addresses. Receive ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml

The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```

!---
!--- Permit DNS over TCP traffic from trusted hosts allowed to the RP.
!---
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
any eq 53
!---
!--- Deny DNS over TCP traffic from all other sources to the RP.
!---
access-list 150 deny tcp any any eq 53
!--- Permit all other traffic to the RP according
!--- to security policy and configurations.
access-list 150 permit ip any any
!--- Apply this access list to the ‘receive’ path.

```



```
ip receive access-list 150
```

* Control Plane Policing

Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

The CoPP example below should be included as part of the deployed CoPP that will protect all devices with IP addresses in the infrastructure IP address range.

```
!---
!--- Feature: DNS over TCP
!---
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 53
!---
!--- Permit DNS over TCP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature.
!---
access-list 150 permit tcp any any eq 53
!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and
!--- Layer 4 traffic in accordance with existing security policy
!--- configurations for traffic that is authorized to be sent
!--- and to infrastructure devices.
!--- Create a class map for traffic to be policed by
!--- the CoPP feature.
!---
class-map match-all drop-tcp-class
  match access-group 150
!---
!--- Create a policy map that will be applied to the
!--- control plane of the device.
!---
policy-map drop-tcp-traffic
  class drop-tcp-class
    drop
```

```
!---
!--- Apply the policy map to the
!--- control plane of the device.
!---
control-plane
service-policy input drop-tcp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```
policy-map drop-tcp-traffic
class drop-tcp-class
police 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature can be found in the documents “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

- CSCtb66963

Symptoms: A SIP call from a call-forwarded phone to a Cisco IOS VoIP gateway is rejected when INVITE contains a comma in the Diversion Header.

Conditions: Example of an inbound SIP invite that contains a Diversion field such as this:

```
---- Received: INVITE sip:15551111111@10.1.134.116:5070 SIP/2.0 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 Remote-Party-ID:
<sip:5555555555@172.27.128.130>;party=calling;screen=yes;privacy=off From:
<sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879?
To: <sip:15551111111@10.1.134.116> Date: Sat, 29 Aug 2009 08:06:56 GMT Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Supported: timer,replaces Min-SE: 1800
User-Agent: Cisco-CCM5.1 Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK,
UPDATE, REFER, SUBSCRIBE, NOTIFY CSeq: 101 INVITE Contact:
<sip:5555555555@172.27.128.130:5070> Expires: 180 Allow-Events: presence
Session-Expires: 1800 Diversion: "Smith, John"
<sip:87007@172.27.128.130>;reason=unconditional;privacy=off;screen=no Max-Forwards: 7
Content-Type: application/sdp Content-Length: 214 ----
```

The IOS gateway will respond back with the following:

```
---- Sent: SIP/2.0 400 Bad Request - "Malformed CC-Diversion/Diversion/CC-Redirect
Header" Reason: Q.850;cause=100 From:
<sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879
Content-Length: 0 To: <sip:15551111111@10.1.134.116>;tag=B8C0430-6C Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 CSeq: 101 INVITE ----
```

Workaround: Modify the diverting name associated with the redirecting device so that it does not contain a comma.

- CSCtb67967

Symptoms: PPP fails at LCP stage with VPDN dial-out calls.

Conditions: This symptom is observed in Cisco IOS Release 12.4T in a dial-out scenario.

Workaround: There is no workaround.

- CSCtb68229

Symptoms: The box crashes within “cns config notify code”.

Conditions: This symptom is observed in the corner case when someone removes “cns config notify diff” from the config while adding other CLIs to the running config by using the method “config replace”. The box can crash.

Workaround: Do not remove “cns config notify diff” using “config replace”.

- CSCtb68539

Symptoms: There may be problems with downloading large packages from remote server to local server.

Conditions: The symptom is observed when the package size is approximately greater than 4KB.

Workaround: Use small packages.

- CSCtb69063

Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:

```
config# username <name of 64 characters> priv <0-15> password 0 <password>
```

Conditions: The symptom is observed if the user name is exactly 64 characters.

Workaround: Configure a user name of less than 63 characters.

Further Problem Description: When some configurations are added, modified, or deleted the **show configuration id detail** command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the “changed by user” field prints unwanted characters.

- CSCtb69796

Symptoms: The tunnel stitching VC may go down, resulting in traffic loss.

Conditions: This symptom is observed when the remote peer is changed with a different MTU, causing the tunnel stitching VC to go down. When the matching MTU is reconfigured, however, the tunnel stitching session does not come back up.

Workaround: There is no workaround.

- CSCtb69859

Symptoms: A Cisco router may crash with the following traceback:

```
0x40A0D7E8 0x40A0C870 0x409D4DC4 0x4098E0AC 0x42655B74 0x40E3CE4C 0x40E3D634
0x40E3DAB8 0x40974B78 0x40974B5C
```

Conditions: This symptom is observed while configuring a DHCP address pool using the **ip dhcp pool TAL_DHCP_vrf_pool** command.

Workaround: There is no workaround.

- CSCtb70102

Symptoms: When SRST and STCAPP are configured and running on the same router, SCCCP-controlled analog phones may be unable to make an outgoing call.

Conditions: This symptom is observed when, upon WAN link failure, the phones register to an SRST gateway.

Workaround: There is no workaround.

Further Problem Description: This symptom occurs due to STCAPP automatically adding a *station-id* parameter under the **voice-port** command in order to save DN information for registration to SRST.

- CSCtb71889

Symptoms: DNS A-answer from IPv4 DNS server (which is supposed to be forwarded to IPv6 side as AAAA-answer) is dropped on NAT-PT routers.

Conditions: The symptom is observed when DNS NAT-ALG is enabled.

Workaround: There is no workaround.

- CSCtb72550

Symptoms: Call Detail Record (CDR) files pushed via FTP are not created on the FTP server.

Conditions: This symptom is observed when the **gw-accounting file** command is configured to point to an FTP server.

Workaround: Push the CDR records locally to the flash instead of to an FTP URL.

- CSCtb72653

Symptoms: The router crashes when unconfiguring a policymap from a virtual interface.

Conditions: This issue is seen only when the interface is a virtual interface and the configuration is changed after the interface flaps.

Workaround: There is no workaround.

- CSCtb72664

Symptoms: 100% ingress packet drop (IQD) with depletion of free IO memory.

Conditions: This symptom is observed in a Cisco 3945 [NM-1A-OC3-POM] <-> [NM-1A-OC3-POM] peer setup. In this or a similar scenario, stressing the OC3 module at the line rate (~84Mbps) with bi-directional traffic will cause this symptom along with depletion of free IO memory.

Workaround: Do not stress the NM-1A-OC3-POM module at the line rate. Stopping or reducing the traffic rate should resolve the depletion of free IO memory.

- CSCtb75294

Symptoms: A router crashes upon bringing up PPP sessions.

Conditions: The symptom is observed if IP pools are configured.

Workaround: There is no workaround.

- CSCtb76775

Symptoms: A Cisco 3900 series router may experience a large IO memory leak.

Conditions: This symptom is observed with IPSec and QoS on a Cisco NM-1A- T3/E3 network module with NME-IPS in promiscuous mode.

Workaround: Run IPS in inline mode.

- CSCtb78266

Symptoms: An incorrect NAS port ID is given when testing IDBless VLAN for PPPoE.

Conditions: The symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 12.4(15)T10.

Workaround: There is no workaround.

- CSCtb79211

Symptoms: A Cisco AS5400XM may process switch all traffic through interfaces. Other platforms may be affected.

Conditions: The symptom is observed if you are running Cisco IOS Release 12.4(20)T or later and the interface is configured for netflow with one of the following feature sets:

- c5400-ik9s-mz
- c5400-ik9su2-mz
- c5400-jk9su2_ivs-mz

Workaround: Disable netflow.

- CSCtb81833

Symptoms: A Cisco router crashes due to a watchdog timeout during interface range port-channel.

Conditions: This symptom is observed on a Cisco router after entering the **interface range port-channel** command with PPPoE configuration.

Workaround: There is no workaround.

- CSCtb82256

Symptoms: A Cisco router may crash.

Conditions: This symptom is observed when all of the following occur:

- Cisco Unified CallManager XML configuration files are downloaded to the router while the router is processing the pri-group configurations
- the **shutdown** and **no shutdown** commands are entered on the voice port and
- the **no ccm-manager** command is entered.

Workaround: Do not shut down the voice port at the time of configuration download.

- CSCtb83353

Symptoms: After an RP switchover, the new active RP log shows many tracebacks and all sessions/tunnels are torn down.

Conditions: The symptom is observed when LNS is configured with 16000 sessions/8000 tunnels (two sessions per tunnel); all sessions with Model D2 QoS. It is seen after an RP switchover.

Workaround: There is no workaround.

- CSCtb83578

Symptoms: A severe memory leak may occur on a Cisco CME router.

Conditions: This symptom is observed on a Cisco CME router with the CCSIP- REGISTER process.

Workaround: There is no workaround.

- CSCtb86203

Symptoms: Degradation occurs when creating and bringing up 1k GRE/IPIP tunnels.

Conditions: This symptom is observed only while scaling up to 1k tunnels.

Workaround: There is no workaround.

- CSCtb86279

Symptoms: Cisco IOS crashes at bootup.

Conditions: The symptom is observed on a Cisco 1941 with 512MB of on-board memory.

Workaround: There is no workaround.

- CSCtb87856

Symptoms: Router can crash with a "%SYS-3-CPUHOG:" when DMVPN is deployed.

Conditions: The symptom is observed when the physical interface (tunnel source) of the router is shut, the routing neighbourship flaps, and memory consumption is increased to the point that there is no free memory left. This causes the router to crash.

Workaround: There is no workaround.

- CSCtb88409

Symptoms: A Cisco router may crash when configuring the object id in config-event-objlist subconfiguration mode.

Conditions: This symptom is observed when entering the **cns config notify** command.

Workaround: There is no workaround.

- CSCtb89424

Symptoms: In rare instances, a Cisco router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

```
hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC
= 0x424ECCE4
```

Conditions: This symptom is observed while using IP SLA.

Workaround: There is no workaround.

- CSCtb89819

Symptoms: A single ping packet with size that is greater than or equal to 1501 bytes will cause a router with an ATM interface to crash.

Conditions: The symptom is observed only when NAT or "ip virtual-reassembly" is configured on an ATM interface.

Workaround: There is no workaround.

- CSCtb90751

Symptoms: FTP and HTTP protocols are not supported for the remote download of FPM packages.

Conditions: The symptom is observed with the remote download of FPM packages.

Workaround: Use TFTP, SCP, or HTTPS.

- CSCtb91412

Symptoms: An IPv6 EIGRP session may go down if one of the IPv6 addresses configured on the interface is deleted.

Conditions: This symptom is observed when more than one IPv6 address is configured on the interface, and one of the those addresses is then deleted.

Workaround: There is no workaround.

- CSCtb91992

Symptoms: A Cisco router may crash with chunk-related errors.

Conditions: This symptom is observed on a router with IOS IPS configured after several hours of traffic.

Workaround: There is no workaround, other than removing IOS IPS.

- CSCtb93855

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml>.

- CSCtb95275

Symptoms: Autocommands configured on VTY line or user-profile are not executing while logging through VTY.

Conditions: The symptom is observed if the privilege level is not configured in the user profile.

Workaround: Explicitly configure user privilege in the user profile.

- CSCtb95801

Symptoms: In certain network setups, every five days the router hangs and the following error message is seen:

```
SYS-2-BADSHARE: Bad refcount in datagram_done
```

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T.

Workaround: There is no workaround.

- CSCtb97176

Symptoms: Router may reload unexpectedly shortly after boot up.

Conditions: This symptom is observed when QoS is configured on a router running Cisco IOS Release 15.0M

Workaround: Disable QoS by removing the service-policy statement applied to all interfaces.

Alternate Workaround: Use a previous Cisco IOS release.

- CSCtb98080

Symptoms: When you attempt to browse to a WebVPN portal you only see a blank page. The router does not send the browser a certificate and the portal login page is not displayed. The command **debug webvpn sdps** logs the following error message:

```
WV-SDPS: Sev 4:sslvpn_tcp_read_notify(),line 1569:No to notify read: already queued[1] 004549:
```

Conditions: The symptom is observed when the SSLVPN process is waiting for an HTTP REQUEST from a client on the port configured using the **http-redirect <port no>** command but the process does not wake up. This can happen because of an unexpected IPC message to the SSLVPN process by another IOS process.

Workaround: Remove **http-redirect** from the WebVPN gateway and reload the device.

- CSCtb98508

Symptoms: A Cisco router may experience a bus error crash.

Conditions: The symptom has been experienced on a Cisco 2851 router that is running Cisco IOS Release 12.4(20)T3 and when "callmonitor" is enabled.

Workaround: There is no workaround.

- CSCtc03750

Symptoms: The following error message can be seen on an SSO switchover:

```
%RF-3-NOTIF_TID: Notification timer extended for the wrong client
```

In addition, the secondary RP reloads continuously after an RP switchover.

Conditions: The symptoms are observed when the router has been scaled with 2000 AToM, 1600 TE tunnels, 100 Ethernet over MPLS over GRE (EoMPLSoGRE) sessions, and 100,000 BGP routes.

Workaround: There is no workaround.

- CSCtc04016

Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW/CUBE may experience high CPU utilization, which causes additional calls through the router to fail.

Conditions: This symptom is observed under rare conditions when SIP- associated processes on the Cisco IOS gateway (as seen when the **show process cpu** command is entered) cause extremely high CPU utilization, which causes further calls through the router to fail.

Workaround: There is no workaround.

Further Problem Description: This symptom occurs due to a SIP “491 Request Pending” and ACK loop between the gateway and a third-party device. This loop most often occurs in environments with a large number of SIP REFER transfers. To determine whether the loop is occurring, enter the **show sip statistics** command and look for the RequestPending value; a high and increasing output count could indicate the SIP loop.

- CSCtc04228

Symptoms: The command **mgcp behavior g729-variants static-pt** is the default and will show up in the configuration. This causes a problem when you save the configuration and downgrade to an earlier Cisco IOS Release where this behavior is not present. There, the command will now be enabled when it was not previously.

Conditions: Using an earlier version of a Cisco IOS Release will enable the command.

Workaround: After downgrading to a lower version where **mgcp behavior g729-variants static-pt** is not the default, configure **no mgcp behavior g729-variants static-pt** to remove the CLI.

- CSCtc04351

Symptoms: The GM router might reload.

Conditions: This symptom is observed if the following conditions are met:

1. Many VRFs are configured on the same GM, each belonging to an individual GETVPN group.
2. All the VRFs are triggered to register with the KS at the same time.
3. While #2 is happening, the **clear crypto gdoi** command is entered on the GM.

Workaround: There is no workaround.

- CSCtc05547

Symptoms: Ping may fail on a Cisco 3845 integrated services router (ISR) or other low-end router where tunnel does not support turbo path.

Conditions: This symptom is observed when L2VPN is configured over tunnel.

Workaround: Do not configure L2VPN over tunnel.

- CSCtc06629

Symptoms: A Cisco router may crash at crypto functions after upgrade to Cisco IOS Release 12.2(33r)XNC.

Conditions: This symptom is observed on a Cisco ASR 1000 Series router after upgrading from Cisco IOS Release 12.2(33r)XNB to Release 12.2(33r) XNC.

Workaround: There is no workaround.

- CSCtc09735

Symptoms: CISCO-ICSUDSU-MIB does not report any values on SNMP query for a Cisco HWIC-1CE1T1-PRI card and its variants.

Conditions: This symptom is observed when querying the CISCO-ISCUDSU-MIB by inserting a Cisco HWIC-2CE1T1-PRI card.

Workaround: There is no workaround.

- CSCtc11521

Symptoms: Invalid pointer value is displayed whenever NVRAM is accessed:

"NV: Invalid Pointer value(460E460C) in private configuration structure"

Conditions: This symptom is observed when upgrading NVRAM from an older version to a newer version.

Workaround: Load a prior working image and backup all files in NVRAM, including the startup-config, to another device or tftp/ftp. Load the new image and enter the **erase/all nvram** command followed by the **write mem** command. NVRAM will now be restored. Copy the backup files back to NVRAM.

- CSCtc12312

Symptoms: PKI might get stuck after 32678 failed CRL fetches, causing IKE to stop processing any further ISAKMP packets.

Conditions: This symptom is observed in Cisco IOS Release 12.4.20T4 and Release 12.2(33)SXH5 when CRL checking is performed.

Workaround: Do not perform CRL checking.

Further Problem Description: Normally, this symptom could take years to manifest in a well-designed environment, but in extreme conditions it could occur within hours.

- CSCtc13085

Symptoms: The keys used in the PI11 code for encrypting and decrypting FPM filters in eTCDF are dummy keys, used for internal testing. Those keys need to be replaced with actual keys for encrypting and decrypting filters.

Conditions: The symptom is observed with the keys used in the PI11 code for encrypting and decrypting FPM.

Workaround: There is no workaround.

- CSCtc13344

Symptoms: Cisco Optimized Edge Routing (OER) experiences a fatal error and is disabled:

%OER_MC-0-EMERG: Fatal OER error <> Traceback %OER_MC-5-NOTICE: System Disabled

Conditions: This symptom is observed when configuring OER to learn the inside prefixes within a network by using the **inside bgp** command.

Workaround: Disable prefix learning by using the **no inside bgp** command.

- CSCtc13664
Symptoms: With an IPv6 Policy Based Routing (PBR) configuration, the route-map clause “set interface null0” may cause a router to crash.
Conditions: The symptom is observed with IPv6 PBR. The trigger traffic is traceroute packets (ping packets will not cause the crash).
Workaround: Configure “route-map” as [set interface loop0].
- CSCtc14156
Symptoms: A router crashes while testing Redial Enhancement feature.
Conditions: This symptom happens during the unconfiguration part of ISDN dialer profile.
Workaround: Wait for a period of 30 seconds before starting the un- configuration.
- CSCtc16399
Symptoms: NIOS watchdog timer times out.
Conditions: This symptom is observed when an MC5727 modem is power-cycled.
Workaround: Reload the router.
- CSCtc16589
Symptoms: A Cisco router may crash when bringing up PPPoE sessions.
Conditions: This symptom is observed when bringing up 1000 PPPoE sessions from two ends, one a client router and the other the equipment of a third-party vendor.
Workaround: There is no workaround.
- CSCtc17162
Symptoms: A Cisco router may crash due to a SegV exception.
Conditions: This symptom is observed on a Cisco 2650XM router running Cisco IOS Release 12.4(15)T10 when VTI is configured inside the EzVPN.
Workaround: Remove the VTI inside the EzVPN.
- CSCtc18562
Symptoms: When Network Address Translation (NAT) of the outside source address is enabled, the static route to the local IP address is installed in the global RIB instead of the VRF RIB.
Conditions: This symptom is observed when enabling NAT of the outside source address using the **ip nat outside source static global-ip local-ip vrf vrf name add-route extendable match-in-vrf** command.
Workaround: Configure a static route within the VRF.
- CSCtc18841
Symptoms: ARP entry of HSRP enters an “incomplete” state with an ip local- proxy-arp configuration even though the device receives an arp reply from the HSRP active router.
Condition: This symptom is observed when “ip local-proxy-arp” is configured on the received arp reply of HSRP, and when the arp reply is received on the vlan interface.
Workaround: Remove the ip local-proxy-arp configuration from the vlan interface, then shut/no shut the vlan interface.
- CSCtc21389
Symptoms: IMA sub-interfaces do not come up.

Conditions: Occurs if the number of PVCs exceeds 255.

Workaround: Do not create more than 255 PVCs.

- CSCtc23003

Symptoms: A Cisco device running Cisco IOS Software may unexpectedly reload with a STACKLOW message.

Conditions: This symptom is observed when the **logging buffered xml** *xml-buffer-size* command is entered to enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer.

Workaround: Disable the XML syslog buffer and return the size of the buffer to the default using the **no logging buffered xml** *xml-buffer-size* command.

- CSCtc23374

Symptoms: A Cisco router may unexpectedly reload with the following message:

```
%SYS-6-STACKLOW: Stack for process BGP Router running low, 0/9000
```

Conditions: This condition is observed when:

1. BGP is configured
2. BGP has learned about multiple networks
3. The **clear ip bgp soft** or other **clear ip bgp** commands are entered, or when BGP-related configurations are removed.

Workaround: There is no workaround.

- CSCtc23465

Symptoms: A Cisco 881 Integrated Services Router (ISR) may pause indefinitely or reload unexpectedly when a DMVPN tunnel interface is configured.

Conditions: This symptom is observed when a DMVPN tunnel interface is configured during the same session in which a **shutdown** command precedes the network-id configuration.

Workaround: Shut down the tunnel after network-id configuration.

Further Problem Description: A traceback followed by a crash typically occurs when multiple interfaces are configured together with the same configuration, even though the traceback can be seen with a single interface. This does not occur once the configuration is saved and the router is reloaded, as the **shutdown** command is always NVGen'ed after the network-id configuration.

- CSCtc23707

Symptoms: A Cisco router may either hang or crash with a watchdog timeout.

Conditions: This symptom is observed when traffic is sent on a router running a pseudo-preemptive process (for example, BFD).

Workaround: Remove the pseudo-preemptive process (for example, the BFD configuration) from the router.

Further Problem Description: To compensate for the absence of the BFD configuration on the router, decrease the time interval between hello packets for the associated routing protocol. Note, however, that this may result in decreased performance. This action is specific to BFD and does not apply to other pseudo-preemptive processes.

- CSCtc24937

Symptoms: The **show cellular** command reports no valid statistics with autoconfig enabled.

```
router#sh cellular 0 radio history all
```

```

router#show cellular 0 all
Hardware Information ===== Modem Firmware Version = Modem Firmware
built = Hardware Version = International Mobile Subscriber Identity (IMSI) = 00000
International Mobile Equipment Identity (IMEI) = Factory Serial Number (FSN) = Modem
Status = Offline Current Modem Temperature = 0 deg C, State = Normal
<..>
Network Information ===== Current Service Status = Normal, Service Error
= None Current Service = Circuit Switched Current Roaming Status = Home Network
Selection Mode = Automatic Country = , Network = Mobile Country Code (MCC) = 0 Mobile
Network Code (MNC) = 0 Location Area Code (LAC) = 0 Routing Area Code (RAC) = 0 Cell
ID = 0 Primary Scrambling Code = 0 PLMN Selection = Automatic Registered PLMN = ,
Abbreviated = Service Provider =
Radio Information ===== Current Band = None, Channel Number = 0 Current
RSSI = -0 dBm Band Selected = GSM 450
Modem Security Information ===== Card Holder Verification (CHV1)
= Disabled SIM Status = OK SIM User Operation Required = None Number of Retries
remaining = 0

```

Conditions: This symptom is observed on Cisco 881 or Cisco 888 router platforms with a 3G wireless interface

Workaround: Test cellular 0 modem-reset command can be used to reset the modem as a workaround.

- CSCtc27454

Symptoms: A Cisco router may crash after displaying the following CPUHOG message for the Crypto ACL process:

```

%%SYS-3-CPUHOG: Task is running for (xxxxx)msecs, more than (xxxx)msecs (xx/x),process
= Crypto ACL.

```

Conditions: This symptom is observed when the DMVPN tunnel is shut down.

Workaround: There is no workaround.

- CSCtc27605

Symptoms: The **show ip route vrf coke** command has no framed route when applied to "ip-vrf".

Conditions: This symptom is observed when a framed-route attribute is downloaded from the AAA server and applied to "ip-vrf."

Workaround: Configure VRF in the user profile where the template was used.

- CSCtc28059

Symptoms: HTTP CORE process might start consuming 99% of a Cisco router's CPU time.

Conditions: This symptom is observed on Cisco ISR routers running Cisco IOS Release 12.4(24)T1 when IOS content-filtering is active and the reputation server is unreachable (that is, timing out during a three-way handshake of the registration SSL connection).

Workaround: Disable the URL content-filtering.

- CSCtc32374

Symptoms: ISDN Layer 1 is deactivated after a reload, and calls fail with a cause code 47 (Resource Unavailable).

Conditions: This symptom is observed when **busyout monitor** is configured and the TEI controller comes up before the monitored interface.

Workaround: Remove the busyout monitor configuration using the **no busyout monitor** command in voice-port configuration mode.

Further Problem Description: Entering the **shutdown** command followed by the **no shutdown** command will bring the PRI Layer 1 to Active and Layer 2 to a MULTIFRAME-ESTABLISHED connection status, but calls still fail with cause code 47.

- CSCtc32375

Symptoms: A Cisco SAF forwarder may crash when the **show eigrp service-family external-client** command is entered.

Conditions: This symptom is observed when an external client attempts to register but omits the client-name attribute in the register message. The registration attempt will be rejected, but subsequent attempts to use the **show eigrp service-family external-client** command will crash the Cisco SAF Forwarder.

Workaround: There is no workaround.

- CSCtc33123

Symptoms: Router may crash when entering the **compress stac** or **compress predictor** command on a PPP-enabled interface.

Conditions: This symptom is observed when stac or predictor compression is configured, or when switching from stac to predictor or from predictor to stac compression.

Workaround: There is no workaround.

- CSCtc35451

Symptoms: A Cisco router used as a SIP gateway unexpectedly sends a register message with the Expires value equal to 0, which causes the SIP trunk to stop working.

Conditions: This symptom is observed when dial-peer is down, even when “no sip-register” is configured.

Workaround: There is no workaround.

- CSCtc36703

Symptoms: Modem calls over BRI are terminated, followed by a channel reset.

Conditions: This symptom is observed when a BRI VIC is used in conjunction with a Cisco Digital Modem PVD Module.

Workaround: There is no workaround.

- CSCtc36826

Symptoms: Unable to detect SIT and disconnect an FXO call.

Conditions: The symptom is observed on an FXO port configured with “supervisory sit us immediate-release” or “supervisory sit us”.

Workaround: Configure “supervisory sit us all-tones”.

- CSCtc37697

Symptoms: A Cisco router pauses indefinitely or reloads unexpectedly.

Conditions: This symptom is observed when the ATM PVC bundle is removed and reapplied, and when OAM is configured on the bundle.

Workaround: There is no workaround.

- CSCtc39592

Symptoms: Classification is broken on an ATM PVC bundle.

Conditions: This symptom is observed only when crypto is applied on an ATM PVC bundle.

Workaround: There is no workaround.

- CSCtc40477

Symptoms: A Cisco router may crash after disabling then re-enabling NBAR on an interface.

Conditions: This symptom is observed when policy-map classification based on NBAR and NAT is configured on the router.

Workaround: Create a dummy subinterface and enable NBAR using the **ip nbar protocol-discovery** command.

Alternate workaround: While migrating on the subinterface, disable NBAR using the **no ip nbar protocol-discovery** command on the old interface only after enabling NBAR on the newly-migrated interface.

- CSCtc42605

Symptoms: Memory leak can be observed when reconfiguring class-map attached to a zone-pair.

Conditions: The symptom can be observed with a router that is running Cisco IOS Release 15.0(1)M0.1.

Workaround: There is no workaround.

- CSCtc42734

Symptoms: A communication failure may occur due to a stale next-hop.

Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.

Workaround: Reload the router.

- CSCtc43507

Symptoms: DSPfarm Transcoding feature is not present in the Cisco IAD 2430, and the following warning message is displayed:

"DSPfarm features are not supported on this platform type."

Conditions: This symptom is observed on the Cisco IAD 2430 when configuring DSPfarm transcoding.

Workaround: There is no workaround.

- CSCtc45177

Symptoms: The "text_start" is not showing up in crashinfo.

Conditions: The symptom is observed with crashinfo data.

Workaround: There is no workaround

- CSCtc45293

Symptoms: Ping fails on a back-to-back AIM-IMA bundle when configuring then unconfiguring precedence on a bundle member.

Conditions: This symptom is observed when a PVC is created using the **atm vc-per- vp number** command and the *number* value entered is greater than 255. The PVC does not come up.

Workaround: There is no workaround.

- CSCtc46174

Symptoms: A Cisco 10000 series router configured for ISG does not limit the number of redirected sessions, which could result in high CPU usage.

Conditions: This symptom is observed on a Cisco 10000 series router running ISG and Cisco IOS Release 12.2(33)SB or Release 12.2(31)SB.

Workaround: There is no workaround.

- CSCtc46304

Symptoms: Ping sweep and application-level traffic fail to go through, and connectivity is subsequently lost.

Conditions: This symptom is observed when BFD and shaping are configured on the SHDSL interface.

Workaround: After connectivity has been lost, flap the link to restore connectivity.

- CSCtc46540

Symptoms: A Cisco router may crash.

Conditions: This symptom is observed when stress traffic is present with an LWE IPS package.

Workaround: There is no workaround.

- CSCtc49228

Symptoms: Memory leak of AAA cursor.

Conditions: Install interface configuration using AAA on PPPoE session (such as lcp: interface-config).

Workaround: There is no workaround.

- CSCtc49391

Symptoms: A Cisco router fails to enroll with the CA server.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(0.6)T.

Workaround: There is no workaround.

- CSCtc51539

Symptoms: A Cisco router crashes with a “Watch Dog Timeout NMI” error message.

Conditions: This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

Workaround: Disable BFD.

- CSCtc51573

Symptoms: CME group pickup or pickup features do not work properly.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T1 when a call is placed to the voice-hunt group.

Workaround: There is no workaround.

- CSCtc54257

Symptoms: PPP fails to establish calls on an AAA dial-out scenario.

Conditions: This symptom occurs in a dial-out scenario with a TACACS server.

Workaround: Use a RADIUS server for AAA Dialout.

- CSCtc55964

Symptoms: The **xconnect** command is missing.

Condition: This symptom is observed in Cisco IOS Release 15.0M under the SVI on a Cisco 2900 series router.

Workaround: There is no workaround.

- CSCtc56812

Symptoms:

1. FW drops packets claiming to match default-class-map
2. FW matches incorrect class-map.

Conditions: Any inspect class with “match class” filter is susceptible to failures.

Workaround: For the following configuration, the filters need to be changed to ensure that the “match class” is the last filter in the class:

```
class-map type inspect match-all C1 match class-map C2 match access-group name
ACL-name
```

should be changed to:

```
class-map type inspect match-all C1 match access-group name ACL-name match class-map
C2
```

- CSCtc57940

Symptoms: A Cisco 2951 ISR G2 may crash when a SIP phone registered to SIP CME parks a call.

Conditions: This symptom is observed on a Cisco 2951 ISR G2 when the following conditions are present:

- call-park system application is configured in telephony-service mode
- a park slot is configured with a timeout limit
- the SIP phone parks a call.

Workaround: There is no workaround.

- CSCtc58917

Symptoms: Dialer idle timeout is not being reset with interesting traffic.

Conditions: This symptom is observed when MPPC compression is turned on.

Workaround: There is no workaround.

Further Problem Description: A call is made from Windows XX client dial-up networking to the NAS. After the call is established and interesting traffic is sent every 30 seconds for 180 seconds, idle timeout is not being reset.

- CSCtc59574

Symptoms: A Cisco 3945 integrated services router (ISR) may crash with HSRP, SNAT, BFD, EIGRP configured.

Conditions: This symptom is observed on a Cisco 3945 ISR with NM-1A-OC3-POM or NM-1A-T3/E3 cards installed when IP NAT is removed or added on a BFD-enabled interface.

Workaround: There is no workaround.

- CSCtc61025

Symptoms: For VPLS autodiscovered pseudowires using FEC129, the label release message is not understood by the peer in Inter-op tests.

Conditions: The symptom is observed when you delete the VFI or shut the attachment circuit to cause the label withdraw message to be sent. The peer will correspondingly send the label release message.

Workaround: There is no workaround.

- CSCtc70423

Symptoms: A Cisco VXML router may experience a memory leak in the Dead process.

Conditions: This symptom is observed on a Cisco AS5350 running Cisco IOS Release 12.4(15)T9 and configured for VXML.

Workaround: There is no workaround.

- CSCtc71922

Symptoms: The **dialer watch-list xx ip a.b.c.d yy.yy.yy.yy** command cannot be unconfigured.

Conditions: This symptom is observed upon entering the **no dialer watch-list xx** command.

Workaround: Use the **no dialer watch-list 2 ip a.b.c.d** command.

- CSCtc73441

Symptoms: A CPUHOG message is observed on the key server (KS) when the **show crypto gdoi ks members** command is executed. As a result of the CPUHOG, the BGP session goes down between the KS and the iBGP neighbor.

Conditions: The symptom is observed on primary or secondary key servers that have more than 1000 group members.

Workaround: There is no workaround.

- CSCtc73759

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323>.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtc75687

Symptoms: Some commands with large outputs allow the use of ctrl-^ to stop the output before completion. This can cause a crash.

Conditions: Unknown at this time.

Workaround: Enter the **no parser command serializer** command.

- CSCtc78200

Symptoms: A Cisco router may crash in `parse_configure_idb_extd_args` routine.

Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

Workaround: As the PPP session is being established on the LNS, Cisco IOS will momentarily use one of the available VTYs from the router. After initial configuration, it is immediately released to the system pool.

If all VTY connections are in use, an RP crash will occur if a new PPP session is established and there are no free VTYs in the system.

To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect using multiple VTY connections at the same time, reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:

```
ip access-list extended VTY_ACL deny ip any any ! line vty 5 9 access-class VTY_ACL in
exec-timeout 1 0 login authentication local1
```

Alternate Workaround: Do not configure “interface range” cli using `ios_config` from `telsh` mode. When in `telsh` mode, use normal “interface cli” in a “for loop.”

- CSCtc79670

Symptoms: A Cisco router crashes @`chunk_free_caller` and displays the following:

```
chunk name is CCE 7 tuple dy
```

Conditions: This symptom is observed when traffic is running through a router that has been configured with Zone-Based Cisco IOS Firewall.

Workaround: Remove Cisco IOS Firewall from the router.

- CSCtc81283

Symptoms: The following error is displayed when attempting to integrate Cisco Unified CCX 8.0 with Cisco Unified Communications Manager Express (CME):

```
AXL_EXCEPTION:Unknown AXL Exception: Exception=org.xml.sax.SAXParseException: The
element type "ISEExtension" must be terminated by the matching end- tag
"</ISEExtension>".
```

Conditions: This symptom is observed when Cisco Unified CCX 8.0 is integrated with Cisco Unified CME.

Workaround: There is no workaround.

- CSCtc81358

Symptoms: The Standby RP reloads after an SSO.

Conditions: The symptom is observed with a scaled L3VPN scenario.

Workaround: There is no workaround.

- CSCtc83838

Symptoms: A memory leak occurs with a SESM request.

Conditions: This symptom is observed if command code “0” is included in the SESM request.

Workaround: There is no workaround.

- CSCtc86342

Symptoms: Inbound SIP calls on an IOS SIP GW/CME fail with 500 Internal Server Error.

Conditions: This symptom is observed when

- Inbound SIP INVITE has multiple VIA headers
- Voice source-group is configured on IOS SIP GW / CME with access-list
- Cisco IOS is Release 15.0(1)XA or Release 12.4(24)SB.

Workaround: Install an earlier version of Cisco IOS, such as Cisco IOS Release 12.4(20)T2.

Alternate Workaround: Remove the voice source-group configuration.

- CSCtc95709

Symptoms: During ISSU upgrade, the standby router may crash and reload after displaying the following error message:

`DATA CORRUPTION-1-DATA INCONSISTENCY or DATA CORRUPTION DATA INCONSISTENCY`

Conditions: This symptom is observed during ISSU upgrade if RPs are in slots between LCs. If RPs are in slots below all LCs, or slots above all LCs, the symptom should not occur.

Workaround: Physically move RPs to the lowest slot numbers, below the LC slot numbers. Moving RPs one by one should allow continued serviceability.

- CSCtc97503

Symptoms: The following error may be seen on the console at bootup:

`Overly long password truncated`

Conditions: This symptom is observed when service password-encryption needs to be configured. This is seen only for the ftp password when the password for ftp is 12 characters or longer. It is not a problem for other passwords specified in the configuration.

Workaround: Use a shorter password.

- CSCtc97687

Symptoms: A mobile router (MR) cannot roam between two interfaces on the same access router or between two different access routers.

Conditions: This symptom is observed on an MR with a single roaming interface roaming between two different interfaces on the access router or between two different access routers.

Workaround: There is no workaround.

- CSCtd00054

Symptoms: Link flap/down on PA-MC-T3E3-EC interface.

Conditions: This symptom is observed when changing encapsulation after reload.

Workaround: Perform an online insertion and removal (OIR) of the PA.

- CSCtd00194

Symptoms: A Cisco 1841 router fails association with EAP authentication of non root bridge.

Conditions: This symptom is observed on a Cisco 1841 ISR running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCtd02154

Symptoms: Three-way conferencing on CME does not work with one PSTN caller, and music on hold does not work for PSTN callers.

Conditions: This symptom is observed on a Cisco IAD 880 series running Cisco IOS Release 15.0(1)M. CME is enabled on the Cisco IAD 88x, and the SIP Trunk is the PSTN access for the Cisco IAD 88x with G.729 codec.

Workaround: Use SIP Trunk with G.711 codec.

- CSCtd07320

Symptoms: Spurious memory access and Traceback is seen @ppp_ipfib_install_punt_adjacency.

Conditions: This symptom is observed when running a conditional debug in a scenario with ISDN and MLP involved.

Workaround: There is no workaround.

- CSCtd13603

Symptoms: A Cisco device may crash after the **show cef switching reinject handles** command is entered.

Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SRE.

Workaround: There is no workaround.

- CSCtd15454

Symptoms: A Cisco router may crash while performing online insertion and removal (OIR).

Conditions: This symptom is observed on a Cisco 7200 NPE-G1 router on PA-GIG in an MPLS environment with traffic.

Workaround: There is no workaround.

- CSCtd16512

Symptoms: Web Cache Communications Protocol (WCCP) redirection cannot be configured with a non-default VRF on a subinterface.

Conditions: This symptom is observed when configuring WCCP redirection with a non-default VRF on a subinterface.

Workaround: There is no workaround.

- CSCtd18510

Symptoms: A Cisco router may crash and display a SegV exception error.

Conditions: This symptom is observed on a Cisco router when OSPF connects the CE and PE routers in an MPLS VPN configuration, and when none of the interfaces are in area 0. This symptom is seen only in Cisco IOS Software versions with the OSPF Local RIB feature.

Workaround: Enter the **no capability transit** command in the OSPF routing processes.

- CSCtd18646

Symptoms: Consult transfer across FXO/FXS trunk cannot be completed.

Conditions: This symptom is observed when a consult call is made across an FXO/FXS trunk. The callerid is incorrect on the sip phone transfer.

Workaround: There is no workaround.

- CSCtd21888

Symptoms: A Cisco router may crash when resetting the mac address of the voice gateway.

Conditions: This symptom is observed on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCtd21969

Symptoms: The following error message for MFIB sub-block occurs:

```
INTERFACE_API-3-NODESTROYSUBBLOCK
```

Conditions: The symptom is observed when running virtual access interfaces when multicast is enabled.

Workaround: There is no workaround.

- CSCtd22063

Symptoms: Call-forward busy/all fails with no H.450 forwards.

Conditions: This symptom is observed on secure IP phones with no H.450 forwards.

Workaround: Configure with H.450 forwards, or configure no supplementary- service media-renegotiate with no H.450 forwards.

- CSCtd26215

Symptoms: A Cisco router reports for no apparent reason that an update is malformed or corrupted. When generating an update, the router reports

```
%BGP-4-BGP_OUT_OF_MEMORY
```

and the BGP resets. The update is not malformed and the router is not running out of memory, but BGP falsely believes that there is no more memory available.

Conditions: This symptom is observed when BGP damping with routemap is configured on a Cisco router that is running Cisco IOS Release 15.0(1)M, Release 12.2 (33)SRE, Release 12.2(33)SRD3, or Release 12.2(33)SRC5.

Workaround: Remove the BGP damping routemap.

- CSCtd26819

Symptoms: A Cisco AS5400 series gateway does not pass cause code in a Progress message to the Cisco Unified Communications Manager (CUCM); therefore, Dialer cannot correctly categorize invalid numbers.

Conditions: This symptom is observed on a Cisco AS5400 series gateway, which currently does not have this capability.

Workaround: There is no workaround.

Further Problem Description: SIT Detection non-standard SIT tones.

- CSCtd30469

Symptoms: A Cisco router may hang.

Conditions: This symptom is observed when reconfiguring NBAR on the subinterface.

Workaround: Ensure that ip nbar protocol-discovery is configured in interface mode, then configure it in subinterface mode.

- CSCtd30625

Symptoms: Getting traceback at config_neighbor_qi.

Conditions: This symptom is observed on a Cisco 7200 platform router.

Workaround: There is no workaround.

- CSCtd31084

Symptoms: GSM-AMR CODEC cannot be disabled on a Cisco MGCP gateway when using iLBC. The CODEC will be selected regardless and then rejected due to lack of license.

Conditions: This symptom is observed under the following conditions:

- iLBC is in use
- GSM-AMR is not licensed for use
- GSM-AMR is in SDP

Workaround: Disable CODEC on the gateway CODEC choice list. Note that this option is not always possible.

- CSCtd31229

Symptoms: The User-Name attribute is missing in all accounting records.

Conditions: This symptom is observed when Multilink PPP (MP) is enabled and making a dialout from NAS to the client.

Workaround: There is no workaround.

- CSCtd31465

Symptoms: An H323 to SIP CUBE may get stuck in a race condition if a reINVITE with delayed media is quickly followed by a reINVITE with early media while still renegotiating the H323 side of the call for the delayed media INVITE. This may lead to one-way or no-way audio.

Conditions: This symptom was observed with the following topology: IP phone---CUCM---H.323 Fast Start---CUBE---SIP---3rd-party SIP server--- CallCenter

Calls flow from the IP phone to the CallCenter hanging off a 3rd-party device. The 3rd-party device re-INVITEs, rapidly, as calls traverse through its menu/IVR system.

Workaround: There is no workaround.

- CSCtd33166

Symptoms: A Cisco router may crash at “parse_call_action_func.”

Conditions: This symptom occurs in “before and after” mode when configuring the Call Home feature.

Workaround: Turn off “before and after” mode.

- CSCtd35091

Symptoms: The input queue on ISG’s access interface gets filled up causing the interface to wedge.

Conditions: The symptom is observed when an L2-connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address to the one used to identify the session. This traffic is dropped and interface wedging is observed.

Workaround: There is no workaround other than a router reload.

- CSCtd35761

Symptoms: Crash is observed on a Cisco Catalyst 6000 with CMM while unconfiguring the pri-group that is provisioned under the controller.

Conditions: This crash is observed when multiple E1/T1 tests are run.

Workaround: There is no workaround.

- CSCtd37710

Symptoms: If FXO lines are used on Cisco Unified Communications Manager Express (CUCME) in Australia and the ephone-dn (octo or dual) receives two calls, if the first caller disconnects from the PSTN when on hold, it causes one-way audio on the second line.

Conditions: This symptom is observed in Australia, since the software interprets normal disconnect as “user busy” when the PSTN disconnects the call on FXO lines only.

Workaround: Configure supervisory custom disconnect cp-tone to force the CME to apply normal call-clearing cause code to disconnect the first call.

- CSCtd42810

Symptoms: PPPoEoA sessions are not coming up because some VCs are in inactive state.

Conditions: This symptom is observed when around 400 PVCs are configured with PPPoEoA sessions.

Workaround: Save the configuration on the LAC, then reload the LAC.

- CSCtd42937

Symptoms: A Cisco router may crash when configuring the **parameter-map type inspect** command

Conditions: This symptom occurs when configuring the **parameter-map type inspect** command in config syntax mode

Workaround: There is no workaround.

- CSCtd43168

Symptoms: A breakpoint exception crash occurs while configuring SNMP traps via Cisco Works after the following errors are displayed:

```
%SNMP-5-WARMSTART: SNMP agent on host <host name> is undergoing a warm start
%SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk #####, data #####.
-Process= "NAT MIB Helper", ipl= 0, pid= 277 -Traceback=
```

Conditions: This symptom is observed after unconfiguring snmp-server, then configuring it again. Commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

Workaround: There is no workaround.

- CSCtd46372

Symptoms: Traceback is observed while configuring fair-queue.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCtd48005

Symptoms: Some dialer sessions are not being freed after all calls are disconnected in an LSDO environment.

Conditions: This symptom is observed when using SGBP (all the remaining sessions are passed to the SGBP peer).

Workaround: Use the **clear dialer sessions** command to free the dialer sessions.

- CSCtd50468

Symptoms: Spurious memory access occurs when configuring DNS operation with IP SLA.

Conditions: This symptom is observed on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCtd51602

Symptoms: A Cisco router may crash or display the following error:

```
%SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk 0, data 0 - Process=
"<interrupt level>", ipl= 1, pid= 12 -Traceback=
```

Conditions: This symptom is observed when enabling SNMP while running traffic.

Workaround: Stop the traffic, enable SNMP, then resume traffic through the router.

- CSCtd51715

Symptoms: Unused links reserved for call-in are sometimes used for dial-out.

Conditions: This symptom is observed when the **dialer reserved- links 4 0** command is configured under the dialer interface.

Workaround: There is no workaround.

- CSCtd51744

Symptoms: Too many BADSHARE messages are seen on reload.

Conditions: This symptom is observed when MFR is in software mode on a Cisco 7200 router and the **wr mem** command is entered, followed by a router reload.

Workaround: There is no workaround.

- CSCtd54296

Symptoms: If the number of Ethernet switch modules installed exceeds the maximum number of switch modules supported by a Cisco 3945, the system will crash if a hw-module oir start is attempted on the Ethernet switch service modules which exceeds the maximum supported configuration.

Conditions: This symptom is observed when the number of Ethernet switch modules installed in the Cisco 3945 exceeds the maximum number of switch modules supported. The following message will be displayed during boot of Cisco IOS Software, if the maximum number of switch ports supported is exceeded:

```
ESWILP_CFG-3-SWITCH_MODULE_COUNT: The number of switching modules in the system
exceeds the supported configuration. The system supports a maximum of 2 switching
modules.
```

When Cisco IOS Software has completed booting, the following will be displayed by the **show diagnostic** command for the Ethernet switch service modules which exceed the maximum switch modules supported:

```
Port adapter is disabled
```

Workaround: There is no workaround.

- CSCtd54873

Symptoms: A Cisco router may crash while resetting the mac address under the voice-gateway system.

Conditions: This symptom is observed on a Cisco 2800 router running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCtd55284

Symptoms: An IP address configured in webvpn context configuration mode may be silently rejected.

Conditions: This symptom is observed with IOS SSLVPN. If the interface does not have an IP address at the time of configuration, the configuration is rejected. Rejection also occurs after a reload if the interface obtains its IP address dynamically.

Workaround: Specify the gateway as an ip address.

- CSCtd60858

Symptoms: While testing dot1x accounting, spurious accesses are seen.

Conditions: This symptom is observed while verifying the attributes in the Access-Request, Access-Challenge, and Access-Accept packets.

Workaround: There is no workaround.

- CSCtd62593

Symptoms: A Cisco router may crash when attaching a policy map configured or unconfigured with **measure type ip-sla group type ip**.

Conditions: This symptom is observed in Cisco routers with Cisco IOS Release 15.1(0.17)T.

Workaround: There is no workaround.

- CSCtd63104

Symptoms: Leaks were seen when configuring and unconfiguring RMI CLIs.

Conditions: Watching and then unwatching a policy by a resource monitor creates the leak.

Workaround: There is no workaround.

- CSCtd63792

Symptoms: Calls may fail to a particular B channel in a PRI with cause code #47 (resources unavailable).

Conditions: This symptom is observed on a Cisco gateway with H323 and PRI and Cisco IOS Release 12.4(15)T10.

Workaround: Busy out the affected B channel.

- CSCtd64492

Symptoms: A subrate interface remains in the “UPDOWN” state when CJ PA is configured in unchannelized mode.

Conditions: This symptom is observed on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCtd66970

Symptoms: IPv6 NHRP support is not included in the -advipservicesk9- feature set.

Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M.

Workaround: Use the -adventerprisek9- feature set instead of the - advipservicesk9- feature set.

- CSCtd67940

Symptoms: A Cisco router may crash while traffic is flowing through the ATM AIM interface.

Conditions: This symptom is observed when a configuration is copied which affects the ATM AIM interface (NAT config in this case) while traffic is flowing through the ATM AIM interface.

Workaround: Stop traffic, copy the configuration, make sure the interface comes up with the new config, then restart traffic.

- CSCtd68173

Symptoms: Outbound DTMF may fail intermittently over a SIP Trunk from Cisco UC 500.

Conditions: This symptom is observed when the following conditions are present:

- Using Cisco IOS Release 12.4.22YB4 or Release 15.0.1XA on Cisco UC 500
- SIP trunk uses RFC2833 for DTMF - Call is outbound from Cisco IP Phone to PSTN over SIP Trunk
- SIP Trunk provider gateway is Sonus GXS (v6.4).

Workaround: Use Cisco IOS Release 12.4(11)XW10 on the Cisco UC 500 if possible; or, SIP trunk provider Sonus GXS gateway should be upgraded to v6.5.5 or higher.

- CSCtd68627

Symptoms: A memory leak occurs at “ikev2_profile_set_laddr.”

Conditions: This symptom is observed while configuring **match local address**.

Workaround: There is no workaround.

- CSCtd68951

Symptoms: A Cisco IOS device with VSA crypto engine acting as an IKEv2 peer may crash when handling several concurrent tunnel setup requests with certificates-based authentication.

Conditions: This symptom is observed when VSA is the crypto engine and several concurrent IKEv2 tunnel requests with certificates-based authentication are being handled. This is not observed with VAM2+ or software crypto engine.

Workaround: There is no workaround.

- CSCtd70439

Symptoms: A packet buffer leak may occur when using the Service Reflect feature.

Conditions: This symptom is observed when an uncoalesced input packet is received by the service reflect VIF in the fast-switching context. The input packet will not be freed after obtaining a new packet buffer and coalescing the input packet into the new buffer.

Workaround: There is no workaround.

- CSCtd72456

Symptoms: Entering the **show snmp pending** command may cause a Cisco switch to crash.

Conditions: This symptom is observed on a Cisco 3750 switch running Cisco IOS Release 12.2(50)SE3 configured to send v3 informs, but may affect other platforms.

Workaround: Do not enter the **show snmp pending** command if you have configured informs in the “snmp-server host” statement.

- CSCtd72647

Symptoms: Severe throughput degradation out an interface occurs when a plain QoS policy map (not hierarchical, with no parent shaper) is applied.

Conditions: This symptom has been observed on Cisco integrated service routers (ISRs) with either HWIC-1FE or HWIC-2FE cards running Cisco IOS Release 12.4(20)T, Release 12.4(22)T, or Release 12.4(24) T. The symptom has not been observed in Cisco IOS Release 12.4(15)T.

Workaround: Use a hierarchical policy map with a parent shaper.

- CSCtd73256

Symptoms: A Cisco Catalyst switch may reload while issuing the **show ip ospf int** command.

Conditions: The symptom is observed when the **show ip ospf int** command is paused while the backup designated router neighbor goes down, for example:

```
c3560sw2#show ip ospf int Vlan804 is up, line protocol is up Internet Address
10.0.0.2/24, Area 0 Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 10.0.0.2,
Interface address 10.0.0.2 --More--
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan804, changed state to down
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on Vlan804 from FULL to DOWN, Neighbor Down:
Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
```

The next line that will be displayed in the “show ip ospf int” output will be the following:

```
Backup Designated router (ID) 10.0.0.1, Interface address 10.0.0.1
```

If at this point you press enter or spacebar to advance the output, the device will reload and the following error message will be shown:

```
Unexpected exception to CPUvector 2000, PC = 261FC60
```

Workaround: There is no workaround.

- CSCtd73923

Symptoms: RSA keys cannot be added to or removed from a token on a Cisco router.

Conditions: This symptom is observed when the **crypto key zeroize rsa** command is entered. The command does not remove the keys, and a “no available resources” message is displayed. Keys cannot then be added to or removed from the token.

Workaround: There is no workaround.

- CSCtd74135

Symptoms: Microsoft Point-to-Point Encryption (MPPE) enforcement may not work on a Cisco router. The router may allow Point-to-Point Tunneling Protocol (PPTP) users to connect without negotiating the MPPE.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.0(1)M even if it is configured with the **ppp encrypt mppe 128 required** command.

Workaround: Using the authentication type of MS-CHAP in place of MS-CHAP-V2 can prevent this issue. The MPPE works fine with the “required” option as well, when used with the authentication type “MS-CHAP.”

- CSCtd74470

Symptoms: Voice ports on gateways configured for E1 R2 intermittently get stuck in the “clearfwd” state and can only be returned to normal operation mode by manual intervention.

Conditions: When the issue occurs, the following states are observed by examining the stuck port with **show** commands:

```
Router#sh vo po su | include clearfwd 0/3/0:1 24 r2-digital up up clearfwd idle y Show
voice trace 0/3/0:1.24 0/3/0:1 24 State Transitions: timestamp (state, event) ->
(state, event) ... 3440023.272 (R2_Q421_IDLE, E_HTSP_SETUP_REQ) -> 3440023.380
(R2_Q421_OG_SEIZE, E_DSP_SIG_1100) -> 3440047.816 (R2_Q421_OG_SEIZE_ACK,
E_R2_REG_ABORT_DIGIT_COLLECT) -> 3440047.816 (R2_Q421_OG_CLR_FWD, E_DSP_DIALING_DONE)
-> 3440048.816 (R2_Q421_OG_CLR_FWD, E_HTSP_EVENT_TIMER) -> 3440050.816
(R2_Q421_WAIT_IDLE, E_HTSP_EVENT_TIMER) -> 3440050.816 (R2_Q421_WAIT_IDLE,
E_DSP_SIG_1100) -> 3440050.820 (R2_Q421_BLOCKED, E_DSP_SIG_1100) -> 3440069.960
(R2_Q421_BLOCKED, E_HTSP_RELEASE_REQ) -> 3440113.512 (R2_Q421_BLOCKED, E_DSP_SIG_1000)
->) ->
```

Workaround: Shut/No shut the controller or Busy Out the channel:

```
Router#sh vo po sum | include clearfwd 0/3/0:1 24 r2-digital up up clearfwd idle y
0/2/0:1 21 r2-digital up up clearfwd idle y 0/2/0:1 29 r2-digital up up clearfwd idle
y 0/2/0:1 30 r2-digital up up clearfwd idle y
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z:

```
Router(config)#control
Router(config)#controll
Router(config)#controller E1 0/2/0
Router(config-controller)#ds0 busyout 21,29,30,24
Router(config-controller) #no ds0 busyout 21,29,30,24
Router(config-controller)#end
Router#sh vo po sum | include clearfwd
Router# -->
```

- CSCtd74943

Symptoms: Multiple PPPoE clients cannot be configured on a single ATM VC.

Conditions: This symptom is observed under all conditions.

Workaround: There is no workaround.

- CSCtd78882

Symptoms: FXO ports can get stuck in offhook state.

Conditions: This symptom is observed when FXO ports are members of a huntgroup where the first member port is disconnected or down. The trunkgroup has max-retry configured and rapid calls are connected and disconnected using the trunkgroup.

Workaround: Unconfigure max-retry. Under each port, configure “timeouts power-denial 0” so that disconnected ports are moved to offhook state and will not be hunted.

- CSCtd80007

Symptoms: The standby routing processor crashes during an SSO when TE auto-tunnel backup is enabled.

Conditions: The symptom is observed during an SSO only on a new standby RP when TE auto-tunnel backup is in use.

Workaround: Disable TE auto-tunnel backup.

- CSCtd81550

Symptoms: Call Forward No Answer does not work for a Cisco Unified Communications Manager (CUCM)-registered IP Phone.

Conditions: This symptom is observed when an RSVP call is made from a SIP gateway to a CUCM-registered IP Phone and the call is set to forward to another IP phone registered to the CUCM.

Workaround: There is no workaround.

- CSCtd83816

Symptoms: A Cisco router crashes at re_multi_match_multiple_tables.

Conditions: This symptom is observed when the parameter map being used by HTTP is modified so that it contains no regex.

Workaround: Do not modify the parameter map being used by HTTP such that there is no regex under it.

- CSCtd84279

Symptoms: No-way audio is experienced in a hardware conference. Entering the **sh voip rtp conn** command will display the remote IP address as “0.0.0.0” instead of displaying the CME’s IP address.

Conditions: When HW conferencing is configured, this symptom is not observed, but it is observed when the router reloads.

Workaround: Save everything under “telephony-service” (all the ephone-dns and ephones) in a notepad file and delete the configuration from the router (including telephony-service). Reload the device and paste in the saved configuration. Reloading the router again will cause the symptom to occur again.

- CSCtd86472

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat>.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd87666

Symptoms: The incoming MLPPP packets via the DSL interfaces are process- switched rather than CEF-switched.

Conditions: This symptom is observed when MLPPP is configured on a Cisco 1861 integrated services router. The symptom does not occur with the same configuration on a Cisco 28xx router.

Workaround: There is no workaround.

- CSCtd87759

Symptoms: Degradation seen in throughput and calls per second (CPS) tests for tcp/udp-based protocols.

Conditions: This symptom is observed when enabling Zone-Based Cisco IOS Firewall inspection for Layer 4/7 protocols.

Workaround: There is no workaround.

- CSCtd88274

Symptoms: Secure conference resource (dspfarm) fails after reload of a Cisco gateway.

Conditions: Secure conference-resources will not register after a gateway reload and shows the status unregistered in CM. The SCCP IOS configuration needs to be deleted then re-inserted to bring the resource back to a registered state. When the condition occurs, entering the **show sccp** command displays “not an active oper state” and “no active callmanager.”

Workaround: There is no workaround.

- CSCtd92203

Symptoms: AAA accounting for voice does not produce the correct values for NASPort for the TDM path. In addition, the calling station ID is missing.

Conditions: This symptom is observed with AAA accounting.

Workaround: There is no workaround.

- CSCtd94704

Symptoms: A Cisco router may reload due to a watchdog timeout in the SCCP application.

Conditions: This symptom is observed when the router is configured for MTP and transcoding for SCCP DSPfarms.

Workaround: There is no workaround.

- CSCtd94947

Symptoms: A Cisco 2851 router running Cisco IOS Release 15.0(1)M and using the onboard HW encryption may stop processing encryption traffic after receiving a multicast packet that matches the encryption policy.

Conditions: This symptom is observed with GETVPN encryption when the time-based anti-replay feature is turned on and when multicast traffic matches a permit statement in the encryption policy.

Workaround: Use software-based encryption by enabling “no crypto engine onboard 0” in the global CLI, or disable the CEF using the **no ip cef** command.

- CSCtd98344

Symptoms: NAT/PAT does not create more than one translation entry for all VRFs after a translation in the first VRF.

Conditions: This symptom is observed when there is more than one VRF.

Workaround: There is no workaround.

- CSCtd99916

Symptoms: After a quick activation/deactivation of a BGP neighbor in the VPNv4 address family, the router can have a unexpected reload. Traceback shows:

```
1#9ef25813351d0da79497b4305144eadc :10000000+5A9860 :10000000+5A9BE4 :10000000+10B9CA0
:10000000+10BEF34 :10000000+421761C :10000000+2AD6FC :10000000+2ADA28 :10000000+2FA91C
:10000000+2FAF84 :10000000+2E748C
```

Exception to IOS Thread: Frame pointer 35233FD8, PC = 1027203C

```
ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = BGP Router -Traceback=
1#9ef25813351d0da79497b4305144eadc :10000000+27203C :10000000+271DAC :10000000+273218
:10000000+2741B8 :10000000+33AE64 :10000000+33B5C4 :10000000+291D2C :10000000+2921C8
:10000000+2928AC
```

Conditions: The symptom is observed whenever an old style multicast update is received and it uses the same AF value as that for VPNv4. Cisco IOS Release 12.2(33)XNE has code that detects this behavior, hence the traceback.

Workaround: Use new-style MDT peering.

- CSCte01303

Symptoms: New Primary KS after failover does not allow KS policy changes.

Conditions: This symptom is observed when a KS failover occurs first, then the policy change is applied on the new primary KS.

Workaround: Apply the policy change in the primary KS once it comes up, then force a KS role re-election by entering the **clear crypto gdoi ks role** in the new primary KS. Once the previously primary KS is restored as the primary KS, apply the policy change.

- CSCte02947

Symptoms: A Cisco IPv6 mobile router may crash.

Conditions: This symptom is observed when IPv6 routing is canceled by entering the **no ipv6 unicast router** command while the IPv6 mobile router is running.

Workaround: Stop the mobile router before entering the **no ipv6 unicast router** command. This can be done by entering the **shutdown** command in the mobile router CLI.

- CSCte03209

Symptoms: On a Cisco 7206/NPE-G2 configured for IRB and L2TP, ingress ARP requests and replies may fail with this message according to “debug arp”:

```
IP ARP: sent req src 10.10.10.2 0000.0c4d.4a20,dst 10.10.10.1 0000.0000.0000 BVI1 IP
ARP rep filtered src 10.10.10.1 000c.85ae.2e00, dst 10.10.10.2 0000.0c4d.4a20 wrong
cable, interface Virtual-Access5.
```

Conditions:

```
bridge irb bridge 1 protocol ieee bridge 1 route ip
interface BVI1 ip address 10.10.10.2 255.255.255.0 ip directed-broadcast
interface Virtual-Templat1 no ip address no peer default ip address ppp
authentication pap chap bridge-group 1 bridge-group 1 spanning-disabled end
interface Virtual-Access5 no ip address no peer default ip address ppp authentication
pap chap bridge-group 1 bridge-group 1 spanning-disabled
```

This symptom is observed on Cisco IOS Release 12.4(15)T7, Release 12.4(15) T9, and Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCte07666

Symptoms: A Cisco router may crash when the TCL script without_completion.tcl is run.

Conditions: This symptom is observed when running the TCL script without_completion.tcl as the script tries to fill in the _cerr_name field with an array that is not sufficiently populated.

Workaround: There is no workaround.

- CSCte08121

Symptoms: Cisco IP phones running firmware that uses SCCP version 17 cannot register to SRST/CME-SRST, or will register but not obtain any lines.

Conditions: This symptom is observed on Cisco routers with Survivable Remote Site Telephony (SRST) and Cisco IOS Release 15.0(1)XA. This is the first image with SCCP version 17 support for SRST.

Workaround: Download the IP phone firmware to a Cisco IOS release image that does not use SCCP version 17. For Cisco 79x1/5/2 phones and Cisco 797x phones, this is 8.4 firmware. For Cisco 7937 phones, obtain a load prior to 1.4(1).

- CSCte14603

A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml>.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-igmp>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte15982

Symptoms: When a Cisco 877 DSL router running Cisco IOS Release 12.4(24)T2 is connected to a 3rd party DSLAM running in 4-wire mode, entering the **clear pppoe all** command may result in a PADS received on one PVC being incorrectly processed on a subinterface associated with a different PVC, which results in two PPPoE sessions transmitting data packets on the same PVC.

Conditions: This symptom is observed under the following working scenario:

```
CPE#show pppoe session 2 client sessions
Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 7 xxxx.xxxx.xxxx
ATM0.38 Di0 Vi1 UP
xxxx.xxxx.xxxx VC: 0/38 UP N/A 8 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
```

After entering the **clear pppoe all** command:

```
CPE#clear pppoe all CPE#show pppoe session 2 client sessions
Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 9 xxxx.xxxx.xxxx
ATM0.40 Di0 Vi1 UP
xxxx.xxxx.xxxx VC: 0/40 UP N/A 10 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
controller DSL 0 mode atm line-mode 4-wire enhanced dsl-mode shdsl symmetric annex B
interface ATM0.38 point-to-point pvc data 0/38 pppoe-client dial-pool-number 1
interface ATM0.40 point-to-point pvc voip 0/40 pppoe-client dial-pool-number 2
interface Dialer0 ip address negotiated encapsulation ppp dialer pool 1 keepalive 60
ppp pap sent-username data@data.com password 0 data
interface Dialer1 ip address negotiated encapsulation ppp dialer pool 2 keepalive 60
ppp pap sent-username voip@voip.com password 0 voip
```

In addition, this symptom is observed under the following conditions:

1. This symptom is not reproducible when running in 2-wire G.SHDSL mode. It is reproducible only when running “line-mode 4-wire enhanced.”
2. The symptom is reproducible in Cisco IOS Release 12.4(15)T7, Release 12.4(15)T10, Release 12.4(20)T, Release 12.4(22)T, Release 12.4(22)T1, Release 12.4(24)T, Release 12.4(24)T1, Release 12.4(24)T2, and Release 15.0(1)M.
3. The symptom can be triggered three ways:

- a. Reload the router
- b. If the reload results in correct behavior, “clear pppoe all.”
- c. If the reload results in correct behavior, any subsequent event which results in both PPPoE sessions being torn down simultaneously.
4. The symptom is not reproducible if any packet layer debugs are enabled, such as “debug pppoe packet” or “debug atm packet.”

Workaround:

1. Reload the router.
 2. After every reload, if the problem is not occurring, configure “debug pppoe packet” on the Cisco 878 router.
 3. After every reload, if the problem is occurring, reload the router until it is not occurring.
- CSCte19478
Symptoms: Entering the **crypto isakmp xauth timeout** command does not seem to have any effect.
Conditions: This symptom is observed when the command is needed for a specific scenario where user input at xauth requires more time than the default timeout value--for example, for rsa authentication (in new pin mode).
Workaround: There is no workaround.
 - CSCte21958
Symptoms: A Cisco router may reload when an L2TP xconnect pseudowire is configured using a pseudowire class that has not yet been defined.
Conditions: This symptom is observed when the following sequence of commands is entered:

```
configure terminal
interface Ethernet0/0.1
encapsulation dot1Q 400
xconnect 10.0.0.1 555 encapsulation l2tpv3 pw-class test
pseudowire-class test
encapsulation l2tpv3
protocol l2tpv3 test
ip local interface Loopback0
vpdn enable
```


This symptom affects all platforms.
Workaround: Define the pseudowire class using the **pseudowire- class** configuration command before referencing that pseudowire class in an xconnect configuration.
 - CSCte23299
Symptoms: A Cisco 877W router is not responding to IPv6 neighbor solicitation.
Conditions: This symptom is observed under normal conditions.
Workaround: There is no workaround.
 - CSCte28777
Symptoms: A line is logged out from the hunt group if the user enables DND, then logs out with extension mobility, logs back in, and disables DND.
Conditions: This symptom is observed when the “ephone-hunt logout DND” option is configured with EM login/logout.
Workaround: Use the “ephone-hunt logout HLog” option instead.

- CSCte30224
Symptoms: A Cisco IOS device may unexpectedly restart when executing a Tcl script that has been compiled into bytecode.
Conditions: This symptom is observed if the Tcl script tries to generate a random number using the **expr rand()** command.
Workaround: Do not use the **expr** command to generate random numbers, or do not compile the Tcl script into bytecode.
- CSCte34718
Symptoms: Network Time Protocol (NTP) may lose synchronization.
Conditions: This symptom is observed on a Cisco 871 router with board rev. C0.
Workaround: Revert to Cisco IOS Release 12.4(15)T3.
- CSCte38945
Symptoms: Unable to get ping reply from the multicast group configured on loopback interface.
Conditions: The symptom can occur when there are multiple routes populated in an interface and the interface goes down. All the routers associated with the interface should be removed, but only one is deleted. This results in the ping failure.
Workaround: Shut down the other interfaces associated with the router and enable it again.
- CSCte39621
Symptoms: Interface is wedged and does not pass traffic.
Conditions: This symptom is observed when the interface is configured for bridge-group and associated to a bvi interface.
Workaround: There is no workaround.
- CSCte42023
Symptoms: In rare timing scenarios, abort may be ignored, resulting in an IOS state machine getting out of sync with module state.
Conditions: This symptom is observed in a very rare scenario of abort being initiated by the user while IOS is simultaneously handling a message from the module that requires the state machine change.
Workaround: Reload the router.
- CSCte42041
Symptoms: Randomly, various DMVPN spokes lose connectivity with the hub.
Conditions: This symptom is observed when NRRP mapping on a spoke does not trigger an IPSec Socket in the SA database. The following error may appear: NHRP: Failed to retrieve NHRP IDB in IF ctrl check
Workaround: Remove and reapply the hub static mapping.
- CSCte53365
Symptoms: The connected EIGRP-owned global addresses are put into the EIGRP topology database after the IPv6 router eigrp <as> process is configured to “no shutdown.”
Conditions: This symptom is observed when the router is reloaded with an IPv6 EIGRP instance configured “shutdown,” then the configuration is changed to “no shutdown.”
Workaround: Configure “shutdown” then “no shutdown” on the interfaces.

- CSCte53732
Symptoms: A Cisco UC520 crashes with memory corruption and frozen console access.
Conditions: This symptom is observed when upgrading from Cisco IOS Release 15.0(1) image XA to XA1 with the default configuration applied.
Workaround: Power-cycle the router. This symptom will not occur after the image has been upgraded.
- CSCte53759
Symptoms: The Cisco 1905 platform is missing the HWIC_1B_U module.
Conditions: This symptom is observed on the Cisco 1905 platform.
Workaround: This module will be supported as part of the M2 rebuild for the Cisco 1905 platform.
- CSCte58425
Symptoms: MAR devices with WMIC cards will not associate in root or non-root mode when the distance between towers is over 2 miles.
Conditions: The symptom is observed with MAR devices with 3205 5Ghz WMIC cards that are mounted on towers and are approximately 2.24 miles apart.
Workaround: There is no workaround.
- CSCte60000
Symptoms: Destination prefix is not collected for IP to MPLS packet flow in netflow aggregation cache.
Conditions: The symptom is observed in a VRF + MPLS setup.
Workaround: Collect prefix in non-VRF + MPLS setup.
- CSCte61096
Symptoms: Traceback is seen on the loading image.
Conditions: This symptom is observed upon loading Cisco IOS Release 15.1(0.25) T.
Workaround: There is no workaround.
- CSCte62782
Symptoms: A Cisco router may crash at bootup after service-policy is applied to ATM PVC, or the router may show spurious memory accesses and subsequently crash on removal or addition of service-policy to ATM PVC.
Conditions: This symptom is observed when hierarchical QoS is applied to ATM PVC.
Workaround: There is no workaround.
- CSCte66046
Symptoms: MDT entries are missing in MPLS forwarding table of P router after OSPF flap on edge router.
Conditions: The symptom is observed on IGP flap in the core.
Workaround: Flap MLDP on P or PE router.
- CSCte71980
Symptoms: IP pool-name downloaded for a particular user is not used to allocate the IP address; instead, a local default pool is being used.

Conditions: This symptom is observed when IP-pool AV pair is downloaded from radius as part of user authorization in a CLI-LAC-LNS scenario.

Workaround: There is no workaround.

- CSCte78562

Symptoms: Trying to run a regexp action on an undefined environment variable generates the following traceback:

```
%SYS-2-FREEBAD: Attempted to free memory at 61, not part of buffer pool
```

Conditions: This symptom is observed if an Embedded Event Manager applet tries to execute a regexp action on an undefined variable.

Workaround: Trying to perform a regexp search on an undefined variable is not allowed. Make sure all arguments to the regexp action are properly defined.

- CSCte81731

Symptoms: A Cisco device may crash after configuring service-policy on an interface.

Conditions: This symptom is observed on a Cisco device in the presence of ICMP filter ACE under the match access-group ACL of a class-map.

Workaround: There is no workaround.

- CSCte81855

Symptoms: The following symptoms occur when a Cisco Voice XML (VXML) gateway reaches 2048 open sockets:

- Dead air on call and call drops
- If customer has survivability TCL enabled in ingress gateway, the call will go to survivability
- Agents can be reserved but voice calls do not reach the agent. Calls to the agent are placed after the original call failed and the call is handled by survivability TCL.
- Errors displayed in the VXML gateway are related to Network Out of Order cause code 38 and ip transfer to 0.0.0.0 ip address failed

Conditions: This symptom is observed in any Cisco gateway, specifically Cisco 2800, Cisco 3800, and Cisco AS53. The symptom occurs in Cisco IOS Release 12.4(15)T6, Release 12.4(15)T7, Release 12.4(15)T8, Release 12.4(15)T9, Release 12.4(15)T10, Release 12.4(15)T11, and Release 12.4(15)T12.

Workaround:

- Make sure the media server and VXML server are reachable
- Make sure all media files requested exist in the media server and that the path to the media file is correct
- Make sure media server backup is configured in the VXML gateway (for example, ip host mediaserver-backup)
- Check the http client process with: show proc cpu | include http client show socket X --> Where X is the id of the http client process showing with the previous command.

If the TCP sockets are getting closed to 2048, shutdown the voice service voip and wait for all the ip calls to finish to reboot the gateway. If this is also an ingress gateway, you will have to re-route the calls to another ingress gateway.

- CSCte83404

Symptoms: A Cisco router may crash and report a bus error.

Conditions: This symptom is observed on a Cisco router using SIP and CME 8.0.

Workaround: Remove the following commands: **nat symmetric role active** and **nat symmetric check-media-src** from sip-ua.

- CSCte87809

Symptoms: Cisco NetFlow Collector does not receive the NetFlow export if it is traversing through a GRE over IPsec tunnel.

Conditions: This symptom is observed on a Cisco 2811 integrated services router (ISR) with Cisco IOS Release 15.0(1)M.

Workaround: There is no workaround.

- CSCte90662

Symptoms: CPU profiling cannot be configured.

Conditions: This symptom is observed under normal conditions.

Workaround: There is no workaround.

- CSCte93101

Symptoms: A Cisco router running Cisco IOS may crash by Watchdog Timeout. The logs prior to the crash will have repeated errors similar to:

```
%SYS-2-INTSCHED: "event dismiss" at level 3 -Process= "OSPF-100 Hello", ipl= 3, pid= 12
```

The process listed is not relevant.

Conditions: This symptom is observed on a router with an interface using HDLC encapsulation with traffic passing. HDLC is the default encapsulation type for serial interface.

Workaround: Change encapsulations away from HDLC using the **encapsulation protocol** command.

- CSCtf00432

Symptoms: A Cisco router may crash while copying a file from the UUT and after checking the Connectivity Fault Management Diagnostics status.

Conditions: This symptom is observed in Cisco routers running Cisco IOS Release 15.1(0.26)T.

Workaround: There is no workaround.

- CSCtf12048

Symptoms: The following Cisco IOS messages may be displayed:

```
%ENVM-3-FAN_SLOW: System detected Sluggish Fan Condition %SMHM-2-SHUTDOWN: Shutdown service module due to a fan failed condition
```

Conditions: This symptom is observed under normal conditions.

Workaround: There is no workaround.

- CSCtf17273

Symptoms: A Cisco router crashes during startup when receiving an AS_SET attribute from its peer.

Conditions: This symptom is observed when the BGP peer sends an AS_PATH or AS4_PATH containing an AS_SET attribute.

Workaround: There is no workaround.

- CSCtf26045

Symptoms: Ignored errors incrementing regularly even with low traffic when the traffic arrives on Multilink PPP, bundling multiple T1.

Conditions: This symptom is observed only when odd byte packets of size 273 arrive on the onboard hdlc driver. This leads to total traffic stoppage, especially if “qos preclassify” is configured on the tunnel interface.

Workaround: There is no workaround.

- CSCtf26271

Symptoms: Cisco SPA 525G2 phone does not register.

Conditions: This symptom is observed when the Cisco SPA 525G2 phone is plugged into the Cisco UC500.

Workaround: There is no workaround.

- CSCtf27187

Symptoms: Traffic stops after doing SPA OIR.

Conditions: This symptom is observed only while doing SPA OIR.

Workaround: Do a SIP OIR; the traffic resumes.

- CSCtf28498

Symptoms: A Cisco router may crash when removing the service policy.

Conditions: This symptom is observed with QoS ACLs containing ICMP ACEs with either TTL, Reflect, or Option field-related entries.

Workaround: Do not use ICMP ACEs with TTL, Reflect or Option field-related entries.

- CSCtf31029

Symptoms: A Cisco HWIC-16A module configured on a Cisco 2900 router for async tunneling may not transmit escape characters (data payload) properly over IP to connected devices even though “escape-character none” is configured under the line.

Conditions: This symptom is observed on Cisco 2901/2911/2921 platforms with Cisco HWIC-8A/16A or HWIC-4A/S modules and running any Cisco IOS release. This symptom does not occur on a Cisco 2951 platform.

Workaround: Use the AUX port.

- CSCtf34853

Symptoms: NS/NA packets are missing when enabling IPv6.

Conditions: This symptom is observed on Cisco routers with onboard GE interfaces.

Workaround: There is no workaround.

- CSCtf37520

Symptoms: Removing bandwidth from policy-map reloads the router.

Conditions: This symptom is observed when two-level policy is configured with bandwidth and shape, then bandwidth is removed.

Workaround: Remove child policy or remove bandwidth in child policy before removing bandwidth in parent policy.

- CSCtf40025

Symptoms: “IP SLAs XOS Event Processor” process hangs and input queue of an interface is stuck.

Conditions: This symptom observed in Cisco IOS Release 15.1T when IP SLA UDP jitter operations are restarted via SNMP.

Workaround: There is no workaround, except for a router reload.



Caveats for Cisco IOS Release 15.1(2)T

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T5, page 282](#)
- [Open Caveats—Cisco IOS Release 15.1\(2\)T4, page 306](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T4, page 306](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T3, page 328](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T2a, page 353](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T2, page 354](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T1, page 367](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T0a, page 371](#)
- [Open Caveats—Cisco IOS Release 15.1\(2\)T, page 372](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(2\)T, page 391](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Resolved Caveats—Cisco IOS Release 15.1(2)T5

Cisco IOS Release 15.1(2)T5 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T5 but may be open in previous Cisco IOS releases.

- CSCsh39289

Symptoms: A router may crash under a certain specific set of events.

Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCso41274

Symptoms: A router crashes or shows the following traceback:

```
% Not enough DSP resources available to configure ds0-group 1 on controller
T1 1/0
% The remaining dsp resources are enough for 14 time slots.
% For current codec complexity, 1 extra dsp(s) are required to create this
voice port.
sip-cme(config-controller)#
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x40C627A8  reading 0x4
%ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C 0x40D72E74
0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
```

Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

Example:

```
sip-cme(config)#controller t1 1/0
sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-imm
sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-immediate-start
```

Workaround: Ensure there are more DSPs in the router than signalling channels.

- CSCso46409

Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM- VPN/SSL-3.

Workaround: There is no workaround.

- CSCsv30540

Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and a traceback are seen.

Conditions: These symptoms are observed when the **show running-config/write memory** command is issued.

Workaround: There is no workaround.

- CSCta11223

Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

Workaround: There is no known workaround.

- CSCtb72734

Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

Workaround: There is no workaround.

- CSCtd15853

Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

Conditions:

- mVPN is configured on the PE router.
- Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

Workaround: There is no workaround.

- CSCte53162

Symptoms: In radius messaging, nas-port-id is not prepended to “acct-session- id” when the **nas-port format e encoding string** command is configured.

Conditions: This symptom is observed when the **nas-port format e encoding string** command is configured.

Workaround: Use the **nas-port format d encoding bits** command.

- CSCtf71673

Symptoms: A Cisco router shows a PRE crash.

Conditions: This issue is seen when the system is configured for PTA and L2TP access and running Cisco IOS Release 12.2(34)SB4 during a pilot phase.

Workaround: There is no workaround.

- CSCtg47129

The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat>

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtg72481
Symptoms: Spurious memory access is seen with QoS configurations.
Conditions: The symptom is observed only when sending the traffic for a while.
Workaround: There is no workaround.
- CSCtg83804
Symptoms: Router crashes when uploading or downloading files via WebVPN.
Conditions: This symptom is observed on a Cisco 870 router, WebVPN, and BVI configuration.
Workaround: There is no workaround.
- CSCth13415
Symptoms: One way audio in call transfer due to 491 response during resume re- INV.
Conditions: The symptom is observed when you have an UPDATE message passing through the CUBE and then a re-INV crossover happens. The re-INV crossover results in a 491 but the 491 is not correctly forwarded by the IPIP GW. This can result in one way audio issues if the crossed over re-INV was changing the media state from hold to resume.
Workaround: There is no workaround.
- CSCth40506
Symptom: A Cisco voice gateway does not have its GigabitEthernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.
Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.
Workaround: There is no workaround.
Further Problem Description: When a voice call is placed, a SIP INVITE is sent:
-- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:
-- ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry: Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
The call, however, is not cleared from the PRI.
- CSCth45432
Symptoms: Traffic that is CEF-switched through the router does not exit Async interfaces.
Conditions: This symptom is observed with CEF enabled and in Cisco IOS Release 12.4(20)T and above with MFI.
Workaround: Disable CEF or downgrade to Cisco IOS Release 12.4(15)T before MFI.
- CSCth61759
Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate the video stream.
Conditions: This symptom is observed in two scenarios:
Scenario 1:

This symptom was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server

1. Call is originated by 7985
2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP "200 OK" response

```
m=video 53722 RTP/AVP 96 97 34 31
  b=AS:1920
  a=rtpmap:96 H264/90000
  a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600
  a=rtpmap:97 H263-1998/90000
  a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1
  a=rtpmap:34 H263/90000
  a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1
  a=rtpmap:31 H261/90000
  a=fmtp:31 CIF=1;QCIF=1
  a=sendrecv
```

3. CUBE sets video m-line to 0 in the SDP of the SIP "ACK" response

```
m=video 0 RTP/AVP 96
```

Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

Workaround: There is no workaround.

- CSCth66177

Symptoms: The standby route processor (RP) triggers an active RP crash.

Conditions: This problem is observed when the standby RP crashes due to a memory parity error.

Workaround: There is no workaround.

- CSCth73173

Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCti01036

Symptoms: A Cisco ASR1000 series router crashes on the Radius Process.

Conditions: This symptom is observed on a Cisco ASR 1000 series router with Radius AAA services enabled. When the Radius server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.

Workaround: Prevent the AAA server from sending empty VSA strings.

- CSCti04919

Symptoms: While unconfiguring and reconfiguring the VRF, PIM neighborship goes down in a specific scenario.

Conditions: This symptom occurs if the PIM MDT GRE tunnel takes more time to come up compared to other interfaces in the VRF.

Workaround: Toggle the default MDT.

- CSCti08811

Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

Conditions: This symptom is observed only with EEM policies.

Workaround: There is no workaround.

- CSCti35326

The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.

The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates the vulnerability is available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-nat>

Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

- CSCti40660

Symptoms: The following message is displayed:

```
%FW-4-GLOBAL_SESSIONS_MAXIMUM: Number of sessions for the firewall exceeds the
configured global sessions maximum value 2147483647
```

Conditions: This symptom is observed when IP SLA is configured along with self zones.

Workaround: There is no workaround.

- CSCti46171

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows: * Memory Leak Associated with Crafted IP Packets * Memory Leak in HTTP Inspection * Memory Leak in H.323 Inspection * Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfb>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-1315 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti48014

Symptoms: A device reloads after executing the “show monitor event <comp> ... all detail” command (where <comp> is an option listed under “show monitor event ?”).

Conditions: This symptom is observed if the configurations are done in the order below,

```
monitor event-trace <comp> stacktrace <depth>
monitor event-trace <comp> size <size value>
```

and any related event gets recorded in between the above two configurations.

Workaround: To avoid the crash, change the order of the above configurations; that is, configure the “size” command first and then configure the “stacktrace” command.

- CSCtj33003

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip>

- CSCtj46670

Symptoms: IPCP cannot complete after dialer interface is moved out of standby mode. CONFREJ is seen while negotiating IPCP.

Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

Workaround: Reload the router.

- CSCtj48387

Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP related errors.

Conditions: This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.

Workaround: There is no workaround.

- CSCtj56551

Symptoms: The Cisco 7600 crashes in a very rare case.

Conditions: This symptom is observed very rarely when route-churn/sessions come up.

Workaround: There is no workaround.

- CSCtj79769

Symptoms: LC crashes.

Conditions: When disabling MLD snooping on an interface or disabling IPv6 multicast in general.

Workaround: There is no workaround.

- CSCtj95685

Symptoms: A router configured as a voice gateway may crash while processing calls.

Conditions: The symptom is observed with a router configured as a voice gateway.

Workaround: There is no workaround.

- CSCtk32975

Symptoms: The system crashes.

Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

Workaround: There is no workaround.

- CSCtl52854

Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

Conditions: The symptom is observed when a multicast server is connected to an EHWIC L2 interface.

Workaround: Connect the multicast server to an on-board gig interface.

- CSCtn04357

Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

```
vlan configuration 161
ip flow monitor flowmonitor1 in
ip flow monitor flowmonitor1 input
```

Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

Workaround 1: Remove the flow monitor configuration.

Workaround 2: Use netflow-v9 export protocol.

Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn16855

Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn58128

Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

Workaround: Ensure “no logging console” is configured.

- CSCtn62287

Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

Workaround: There is no workaround.

- CSCtn65060

Symptoms: A Cisco device crashes.

Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL”.

Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.

- CSCtn65116

Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB or later. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, e.g.: 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). It is seen with the following process:

1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
2. The allocated label changes from 16 to 17, e.g.: due to interface flapping or BGP attribute change.
3. However, before the BGP import happens, a more specific prefix (e.g.: 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, RT policy.

Workaround: Remove RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCtn74673

Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.

Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.

Workaround: There is no workaround other than line card reload.

- CSCto55643

Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

Workaround: There is no workaround.

- CSCto63268

Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

Workaround: Remove the EVM or disable DSP sharing.

- CSCto72480

Symptoms: The output of the **show mfib linecard** command shows that line cards are in “sync fail” state.

Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

Workaround: If this issue is seen, using the **clear mfib linecard slot** command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto72629

Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto72927

Symptoms: Configuring an event manager policy may cause a Cisco router to stop responding.

Conditions: This issue is seen when a TCL policy is configured and copied to the device.

Workaround: There is no workaround.

- CSCto99523

Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

Conditions: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

Workaround: There is no workaround.

- CSCtq04117

Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running.

Conditions: This symptom occurs under the following conditions:

1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

Workaround: Use the **clear ip route vrf x *** command.

- CSCtq12007

Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less severe; you may see one every other packet drop, until the next rekey or tunnel reset.

Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq21234

Symptoms: Label is not freed.

Conditions: The symptom is observed after shutting down the link.

Workaround: There is no workaround.

- CSCtq24557

Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

Conditions: The symptom is observed in a large scale scenario.

Workaround: There is no workaround.

- CSCtq24733

Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.

Conditions: The symptom is observed with MRCP is enabled.

Workaround: There is no workaround.

- CSCtq32896

Symptoms: LSM entries stop forwarding traffic.

Conditions: This symptom is observed after Stateful Switchover (SSO).

Workaround: There is no workaround.

- CSCtq36153

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows: * Memory Leak Associated with Crafted IP Packets * Memory Leak in HTTP Inspection * Memory Leak in H.323 Inspection * Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfb>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-0387 has been

assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq45553

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

* Memory Leak Associated with Crafted IP Packets * Memory Leak in HTTP Inspection * Memory Leak in H.323 Inspection * Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfb>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-0388 has been

assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq49325

Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. If a particular path is threaded to be sent - in this case it is scheduled for a reply message - the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the

paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq55173

Symptoms: A device that is configured with NAT crashes. SIP appears to be translated through NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

Workaround: There is no workaround.

- CSCtq58383

Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq59923

Symptoms: OSPF routes in RIB point to an interface that is down/down.

Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

Workaround: Configure “ip routing protocol purge interface”.

- CSCtq62759

Symptoms: CLNS routing table is not updated when LAN interface with CLNS router is configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when ISIS ages out the stale routes.

Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq75008

Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

Conditions:

- The Cisco 7206 VXR works as a server for L2TP over IPsec.
- Encryption is done using C7200-VSA.
- More than two clients are connected.

If client sessions are kept up for about a day, the router crashes.

Workaround: There is no workaround.

- CSCtq77274

Symptoms: FXS phones are not recognized as SCCP endpoints.

Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

Workaround: There is no workaround.

- CSCtq78217

Symptoms: A router crashes with the following information:

System returned to ROM by address error at PC 0xFFFFFFFF, address 0xFFFFFFFF

Conditions: The symptom is observed with CUBE + SIP.

Workaround: There is no workaround.

- CSCtq80648

Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

For example:

```
interface Ethernet1/0
  vrf forwarding vpn1
  ipv6 address 1::1/64
!
router bgp 65000
  address-family ipv6 vrf vpn1
    neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq83629

Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

Workaround: Line card reload is required to resolve the problem.

- CSCtq85728

Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.

Workaround: There is no workaround.

- CSCtq88777

Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq92182
 Symptoms: An eBGP session is not established.
 Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.
 Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.
- CSCtq92940
 Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.
 Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.
 Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.
 Further Problem Description: Please see the original bug (CSCtl19967) for more information.
- CSCtq96329
 Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
 Conditions: This symptom can happen only when bgp deterministic-med is configured.
 The following releases are impacted:
 - Cisco IOS Release 15.0(1)S4
 - Cisco IOS Release 15.1(2)T4
 - Cisco IOS Release 15.1(3)S
 - Cisco IOS Release 15.2(1)T
 Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.
 It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.
 Further Problem Description: If deterministic med is enabled, withdraws are not sent.
- CSCtr04829
 Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.
 Conditions: This symptom occurs when the hardware address is zero.
 Workaround: There is no workaround.
- CSCtr11620
 Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.
 Conditions: This symptom is observed when a Cisco 2911 is used.
 Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr15891

Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

Workaround: There is no workaround.

- CSCtr18574

Symptoms: H323-H323 video calls fail with cause code 47.

Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:

```
Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
cch323_send_passthru_out: Send passthru message retcode 15
```

Workaround: There is no workaround.

- CSCtr26373

Symptoms: Interface bounces and, after coming back up, hangs and does not pass traffic. The rx ring is stuck and it may be observed that all packets coming into the interface are counted as “input errors”.

Conditions: This has been observed on onboard GE interfaces of Cisco 39xx and Cisco 2951 routers. It may be seen at random times and has thus far been observed to happen after an interface bounce. The interface will still show “up/up” in the **show interface** output.

Workaround: Bounce the interface again to restore service.

- CSCtr28857

A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr29338

Symptoms: A router crashes.

Conditions: The symptom is observed after an %ISDN-6-DISCONNECT message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

Workaround: There is no workaround.

- CSCtr44686

Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
  class type inspect smtp SMTP_L7_C1
    reset
policy-map type inspect smtp SMTP_L7_P2
  class type inspect smtp SMTP_L7_C2A
    reset
  class type inspect smtp SMTP_L7_C2B
    reset
```

Conditions: The symptom is observed with the above maps.

Workaround: Replace “reset” with “log”.

- CSCtr45608

Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr46123

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

- CSCtr49064

The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh>

- CSCtr51926

Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

Conditions: The symptom is observed when a service-policy is applied on the main interface.

Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y
  ipv6 enable
```

Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z
  no ipv6 address
  ipv6 address ...
```

- CSCtr54269

Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr54327

Symptoms: A Cisco router may crash due to a SegV exception or may have spurious access when a fax comes in.

Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the “a=silenceSupp:off” option is set in SDP.

Workaround: Disable fax by going into the “voice service voip” mode and configuring the **fax protocol none** command.

- CSCtr58140

Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

Workaround: There is no workaround.

- CSCtr79347

Symptoms: A router crashes at BGP task without a BGP configuration change or BGP neighbor up/down event.

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
Traceback summary % 0x80e7b6 : __be_bgp_tx_walker_process % 0x80e3bc :
__be_bgp_tx_generate_updates_task % 0x7f8891 : __be_bgp_task_scheduler
```

Conditions: No conditions but this is a rarely observed issue.

Workaround: There is no workaround.

- CSCtr86328

Symptoms: A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.

Conditions: Cisco IOS device configured for clientless SSL VPN.

Workaround: None.

Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C>

CVE ID CVE-2012-1344 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr86437

Symptoms: NAT-PT function does not work properly after an interface flap occurs.

Conditions: The symptom is observed when you configure NAT-PT on the router.

Workaround: Reconfigure "ipv6 nat prefix."

- CSCtr88739

Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove "import-route target" and reconfigure route-target.

Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCtr91106

A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 8.5/7:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:I/C/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-0384 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr97640

Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

Conditions: None.

Workaround: None--Physically securing the router is important.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.9/1.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C> CVE ID CVE-2011-3289 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts16285

Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts28315

Symptoms: A DHCP PD request does not accept a specific server.

Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

<http://tools.ietf.org/html/rfc3633#section-10>

A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

Workaround: There is no workaround.

- CSCts33952

Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

Workaround: There is no workaround.

- CSCts38429

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike>

Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

- CSCts39535

Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts40771

Symptoms: Device goes into a hang state and requires a power cycle. If “scheduler isr-watchdog” is configured, the device will crash and reload the system.

Conditions: This issue has been seen with “ip nbar protocol-discovery” configured on tunnel interfaces.

Workaround: Remove “ip nbar protocol-discovery” from the device.

- CSCts59014

Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

Workaround: There is no workaround.

- CSCts64539

Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts70790

Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

Workaround: Remove and re-add the **neighbor default-originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts76410

Symptoms: Tunnel interface with IPsec protection remains up/down even though there are active IPsec SAs.

Conditions: The symptom is observed during a rekey when the IPsec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts80643

Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

A workaround is available to mitigate this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp>

- CSCtt02313

Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

Workaround: There is no workaround.

- CSCtt11210

Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt17879

Symptoms: The **bgp network backdoor** command does not have any effect.

Conditions: This symptom occurs:

- On 64-bit platform systems.
- When the network is learned after the backdoor has been configured.

Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt20215

Symptoms: Controller goes down after reload.

Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

Workaround: Unplug/plug the cable, or reset link from PBX side.

- CSCtt94391

Symptoms: A Cisco wireless router may unexpectedly reboot due to a bus error with the following error leading up to the crash:

```
ASSERTION FAILED: file '../dot11t/t_if_dot11_hal_ath.c', line XXXX
```

Conditions: This issue relates to the wireless on the router. This crash can be seen on the following platforms: Cisco 870W, 1800W, UC500W, and 2800 and 3800 routers with HWIC-AP. The crash is only seen when an iPhone 4S is connected to the router. The crash has most commonly been triggered by running a video call application on the phone, but there may be other triggers. Other than the wireless configuration and other generic configurations needed to provide connectivity to the router, no other specific configuration is needed to see the crash.

Workaround: No workaround on the router. However, this issue is not seen with an iPhone 4s running iOS 5.1. The issue is only seen on iOS 5.0.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C>

CVE ID CVE-2012-1327 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtw45055

Symptoms: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault, if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session Neighbor deleted
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
```

Exception to IOS Thread:

Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler

The scheduler process will attempt to reference a freed data structure, causing the system to crash.

Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

Workaround: There is no workaround.

- CSCtw99290

Symptoms: The source or destination group-address gets replaced by another valid group-address.

Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

Workaround: There is no workaround.

- CSCtx09973

Symptoms: Voice quality on the network deteriorates after 10 minutes.

Conditions: This symptom is observed when voice traffic is not classified properly and is classified as web or other kind of traffic.

Workaround: There is no workaround. However, use ACL to correctly tag the traffic.

- CSCtx29543

Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

Conditions: This symptom occurs under the following conditions:

1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
2. A default route exists.
3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

The router may now crash when doing **show ip route** command or when default route is updated.

Workaround: There are two possible workarounds:

1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx32628

Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

- BGP full mesh is configured.
- BGP cluster-id is configured.
- **address family vpnv4** is enabled.
- **address family ipv4 mdt** is enabled.

- The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx38806

Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

The problem affects Firefox also (version 10.0.1) displaying the following message:

"The page isn't redirecting properly"

Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.

Workaround: Any of the following workarounds will work:

1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
2. Uninstall the update.
3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

```
webvpn gateway gateway name ssl encryption rc4-md5
```

4. Use AC 2.5.3046 or 3.0.3054.
5. Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:

"Connection attempt has failed due to server communication errors. Please retry the connection"

The AnyConnect event log will show the following error message snippet:

```
Function: ConnectIfc::connect Invoked Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx88093

Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.

Conditions: This symptom occurs while using the "dialer-list x protocol ip deny" command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.

Workaround: Use the method that follows to define interesting traffic instead of "dialer-list x protocol ip deny":

```
access-list x protocol ip deny
dialer-list 1 protocol ip list x
```

- CSCty43587

Symptoms: Crash observed with memory corruption similar to the following:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
dealloc XXXXXXXX
```

Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(2)T4

Cisco IOS Release 15.1(2)T4 is a rebuild release for Cisco IOS Release 15.1(2)T4. The caveat in this section is open in Cisco IOS Release 15.1(2)T4. This section describes only select open caveats.

- CSCtq96329

Symptoms: Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

Conditions: This symptom can happen only when “bgp deterministic-med” is configured.

The following releases are impacted:

- Cisco IOS Release 15.0(1)S4
- Cisco IOS Release 15.1(2)T4
- Cisco IOS Release 15.1(3)S
- Cisco IOS Release 15.2(1)T

Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

Resolved Caveats—Cisco IOS Release 15.1(2)T4

Cisco IOS Release 15.1(2)T4 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T4 but may be open in previous Cisco IOS releases.

- CSCso33003

Symptoms: If a child policy is attached to a parent policy twice, the router will reload if the child policy configuration is removed.

Conditions: The parent policy needs to be attached to the target interface.

Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCtb24959

Symptoms: The router may crash while clearing a large number of RP mappings.

Conditions: This symptom occurs when you configure the router as an RP agent and candidate RP for a large number of RPs. This issue is seen when you run the **clear ip pim rp-map** command several times.

Workaround: Do not run the **clear ip pim rp-map** command several times in succession.

- CSCtb74547

Symptoms: A Cisco ASR 1000 DMVPN HUB reloads at the process IPSEC key engine.

Conditions: This symptom is observed when the “Dual DMVPN with Shared Tunnel-Protection” feature is enabled and the interface is shut down and brought up again.

Workaround: There is no workaround.

- CSCtd23069

Symptoms: A crash occurs because of a SegV exception after configuring the ip virtual-reassembly command.

Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCte89130

Symptoms: Router experiences a memory leak.

Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).

Workaround: There is no workaround.

- CSCtf32100

Symptoms: Packets are dropped.

Conditions: This symptom is observed with router-destined traffic on an interface with VRF and crypto map configured, when the hardware is 7200 G2 with VSA.

Workaround: There is no workaround.

- CSCtf39056

Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.

Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
#####
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
#####
```

- CSCtf41721

Symptoms: A DMVPNv6 hub might crash upon doing a shut/no shut on the tunnel interface of the other hub.

Conditions: This symptom is observed with the following steps:

1. Configure DMVPNv6 with two hubs and two spokes.
2. Hub 2 tunnel is shut and unshut.
3. Hub 1 crashes.

Workaround: There is no workaround.

- CSCtg59328

Symptoms: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

Conditions: This symptom is observed when the following tasks are completed:

- Bring up a PPPoE session and ensure that it is synced to standby.
- From the PPPoE client run the **no ip address** command, followed by the **ip address negotiated** command under the Virtual-template interface.
- As part of the **no ip address** command, the session would first go down on both active and standby. The **ip address negotiated** command would then trigger IPCP renegotiation and the session would come up on active. On standby, the session remains down and the new IP address is not synced.

Workaround: There is no workaround.

- CSCtg72652

Symptoms: On Cisco 2900 series routers, the following warning message might display on the console:

```
%ENVMON-1-POWER_WARNING: : Chassis power is not good in the PSU 1
```

Conditions: Under rare conditions, the power supply sometimes sends a false alarm status to the system, even though the system power is working fine.

Workaround: There is no workaround.

- CSCtg84969

Symptoms: The output of the **show ip mfib vrf vrf-name verbose** command may show the line “Platform Flags: NP RETRY RECOVERY HW_ERR”, and multicast traffic may not be hardware switched.

Conditions: This symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSOs. When the issue occurs, the output of the **show ip mfib vrf vrf-name verbose** command on the standby SP will show some lines preceded with “###” where an interface name is expected.

Workaround: There is no workaround.

- CSCtg89555

Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

Conditions: This symptom is observed when configuring an IP address after multicast has been configured on a dot1Q interface.

Workaround: Performing a shut/no shut of the interface will fix the problem.

- CSCtg91572

Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

Workaround: There is no workaround.

- CSCth01526

Symptoms: The MDT interface is deactivated and activated after an SSO.

Conditions: This symptom occurs after an SSO, when the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

Workaround: There is no workaround.

- CSCth08505

Symptoms: PPPoE sessions may not sync to the standby-RP.

Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

Workaround: Reloading the standby-RP may resolve this issue.

- CSCth11006

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>

- CSCth20018

Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, **no interface g0/0.100** or **no interface atm0/0.100**) may sometimes crash the system.

Conditions: This symptom occurs during basic configuration.

Workaround: Do not unconfigure a subinterface.

- CSCth26441

Symptoms: Non-broadcast Ethernet frames are dropped by the Gig1/0 controller that connects to the NME module.

Conditions: This symptom is observed when xconnect is configured on a subinterface and 802.1q trunking is used to connect to the NME module.

Workaround: There is no workaround.

- CSCth36114

Symptoms: A crash is seen after executing the **write memory** command via SDM.

Conditions: The symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

Workaround: Use Cisco IOS 12.4 versions.

- CSCth37092

Symptoms: A crash is observed in the PKI-HA feature when the standby tries to sync up with the active router.

Conditions: This symptom occurs when the PKI server is created on the active router with a “database archive password” configuration, and the PKI server is cloned on the standby. Soon after, the active router crashes.

Workaround: There is no workaround.

- CSCth45731

Symptoms: PPPoE sessions get synced partially to the standby RP and later never get cleaned up. The **show** command for the sessions looks on a standby RP like the following:

```
Sby#show ppp all
Interface/ID  OPEN+ Nego* Fail-      Stage      Peer Address      Peer Name
-----
--
0xB400008A LCP+ CHAP+ IPV6CP+ Undefined 0.0.0.0
```

The peer address is 0 and the interface will show the PPP handle instead of the virtual interface of PPP.

Conditions: This symptom is seen when IPCP is getting renegotiated and terminated before the full session sync is done for the upcoming PPPoE session.

Workaround: There is no workaround.

- CSCth46888

Symptoms: When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.

Conditions: This symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.

Workaround: There is no workaround.

- CSCth58576

Symptoms: The router crashes with traceback, indicating `cce_dp_named_db_sip_free_token_results_data`.

Conditions: This symptom occurs with Cisco IOS Release 15.1(2)T or later releases. This issue is seen when the device is configured with a zone-based firewall and has SIP Application inspection configured. In addition, the device is configured with “crypto” and “ip virtual-reassembly”.

Workaround: There is no workaround.

- CSCth64271

Symptoms: Routers in redundant configuration end up in Manual Swact = disabled.

Conditions: This symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCth66251

Symptoms: You are not able to configure a policy-map for the second time in a Cisco 860 router. An “internal data base error” message is seen.

Conditions: This symptom is observed when configuring a policy-map for the second time, and with a Cisco 860 router.

Workaround: There is no workaround.

- CSCth74953

Symptoms: The SPI value is shown as 0x0; hence, the ipsec sa validation is failing.

Conditions: This symptom is observed when the crypto profiles are being applied. The symptom is not observed with simple crypto maps.

Workaround: There is no workaround.

- CSCth85294

Symptoms: A PIM neighborhood is not established with the remote PE and RP for the MVRFs.

Conditions: This symptom is observed with traffic, after removal and restoration of MVRFs. Traffic does not flow properly since the PIM neighborhood is not established with the remote PE and RP for those MVRFs.

Workaround: There is no workaround.

- CSCth87458

Symptoms: Memory leak is detected in ssh_buffer_get_string.

Conditions: This symptom occurs when you use test tool Codenomicon to test SSH verification against UUT (SSH-Server test). After the test, the memory leak is seen in ssh_buffer_get_string.

Workaround: There is no workaround.

- CSCti06686

Symptoms: On the Cisco 2900, the async interface drops all outbound packets.

Conditions: This symptom is observed with data packets that are exiting the async interface through the CEF path.

Workaround: Disable hardware framing under the async interface using the hidden command **no ppp microcode**.

- CSCti07805

Symptoms: The router reloads @sipSPIUpdSrtpSession.

Conditions: This symptom is observed during Hold/Resume on a basic SRTP call with Cisco IOS Release 15.1(2.3)T.

Workaround: There is no workaround.

- CSCti18615

Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP being out of sync with the active RP. The A and F flags are missing from the multicast forwarding base entries.

Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, and when the router is in HA mode SSO and is reloaded from the RP.

Workaround: Perform a shut/no shut of the affected interfaces.

- CSCti22544

Symptoms: IKE fails to come up while using RSA signature. PKI debugs show the following message:

```
PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
```

Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example, crypto pki trustpoint yni-u10 enrollment url http://yni-u10:80 vrf coke.

Workaround: There is no workaround.

- CSCti36310

Symptoms: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attributes are pulled by SNMP.

Conditions: This symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

Workaround: There is no workaround.

- CSCti48483

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>

- CSCti48504

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCti64685

Symptoms: Users may not be able to configure SLA MPLS configuration.

Conditions: This symptom occurs when the router is booted up and may be random.

Workaround: There is no workaround.

- CSCtj05903
Symptoms: Some virtual access interfaces are not created for VT, on reload.
Conditions: This symptom occurs on scaled sessions.
Workaround: There is no workaround.
- CSCtj23189
Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.
Conditions: This symptom occurs only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with three classes: one with 16kbps, the second one with 1Mbps, and the third one with 99Mbps.
Workaround: There is no workaround.
- CSCtj30155
Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
 - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
 - ICMPv6 Packet May Cause MPLS-Configured Device to Reload
 Cisco has released free software updates that address these vulnerabilities.
Workarounds that mitigate these vulnerabilities are available.
This advisory is posted at
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>
- CSCtj35792
Symptoms: The onboard GE on a Cisco 3900 (driver PQ3_TSEC) with “media-type sfp” goes to 1000/HD when it is connected by fiber to a gig port that is not doing autonegotiation.
Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation.
Workaround: Configure autonegotiation on the other side, if possible.
Further Problem Description: It is impossible to disable autonegotiation on the Cisco 3900 because of CSCth72105.
The Cisco 3945E has an issue with autonegotiation in Cisco IOS Release 15.1(1)T2. This issue is not seen in Cisco IOS Release 15.1(1)T and Cisco IOS Release 15.1(4)M.
- CSCtj36521
Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.
Conditions: This symptom is observed only if IPv6 CEF is enabled at the same time.
Workaround: Make sure that IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.
- CSCtj84234
Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

```
route-map <RM name>
  match ip address <acl>
  set ip next-hop <NH1> <NH2>
```

Workaround: There is no workaround.

- CSCtj87846

Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtj94297

Symptoms: The “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

Conditions: This symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRP.

Workaround: Use the **clear ip mroute** command in the affected mroute.

- CSCtk02814

Symptoms: The **show pppoe throttled subinterfaces** command output is truncated, and does not show throttled ATM VC or QinQ subinterfaces during throttling.

Conditions: This symptom occurs when pppoe throttling is configured and active.

Workaround: There is no workaround.

- CSCtk46363

Symptoms: A device running Cisco IOS and acting as a DHCP server crashes.

Conditions: This symptom is observed when a client requests a specific IP address.

Workaround: Disable duplicate address detection check using the **ip dhcp ping packet 0** command.

- CSCtk67073

The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla>

- CSCtk74660

Symptoms: The Network Time Protocol (NTP) tries to resync after the server clock changes its time and after the NTP falls back to the local clock.

Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

Workaround: There is no workaround.

- CSCtl00467
Symptoms: A Cisco router crashes.
Conditions: This symptom is observed when call monitoring is enabled and the “conference call” feature is used.
Workaround: There is no workaround.
- CSCtl05684
Symptoms: Xauth user information remains in the **show crypto session summary** command output.
Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different usernames during P1 rekey. This issue is seen when NAT is used in the VPN path.
Workaround: Use the ave-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.
- CSCtl43156
Symptoms: When using a BVI interface configured for IPv6 on a Cisco ISR-G2 series router, IPv6 neighbors are never discovered over the BVI. Neighbors will never be seen in the **show ipv6 neighbors** command output and all traffic to/through the BVI will fail.
Conditions: This symptom occurs when IPv6 is configured on Cisco ISR-G2 router images running on the “data9” package.
Workaround: Use the “uck9” technology package, where the IPv6 feature is already present.
- CSCtl45684
Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

```
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
```


Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.
Workaround: There is no workaround.
- CSCtl67079
Symptoms: The following error message is seen on a Cisco router with HWIC_1GE_SFP inserted:

```
%HWIC_1GE_SFP-3-INTERNAL_ERROR: GigabitEthernet0/0/0 SNMP high capacity
counter register failed
```


Conditions: This symptom is observed during bootup.
Workaround: There is no workaround.
- CSCtl94813
Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analog phone on the VG224 attends a conference bridge. It causes one-way audio.
 - When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen.
 - For the same call, the PCM trace shows no audio in the RIN stream.
Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

```
*Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx:
Got RX stats
```

```

Packet details:
  Packet Length=188, Channel Id=1, Packet Id=200
  RX Packets=0: Signaling=0, ComfortNoise=0
  Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms)
  Packet Counts: OOSquence=0, Bad header=0, Late=0, Early=0Receive
inactive duration=129(ms)

```

Workaround: Downgrade the Cisco IOS to Cisco IOS Release 12.4(4)T8.

- CSCtl95752

Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.

Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.

Workaround: There is no workaround.

- CSCtn08208

Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.

Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.

Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.

- CSCtn08258

Symptoms: The router crashes.

Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T2 and Cisco IOS Release 15.1(3)T1 when SIP calls are made.

Workaround: There is no workaround. However, this issue is not seen in Cisco IOS Release 15.1(4)M.

- CSCtn10922

Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn12119

Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn19178

Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf “A” and a new local label will not be reassigned.

Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf “B”, including:

- The vrf interface, for example, **no interface Gi1/0/1.430**.
- The same vrf process, for example, **no router ospf process id vrf vrf name**.

Run the following commands to verify whether you are facing this issue:

- **show ip bgp vpnv4 vrf A subnet** (this is for the working vrf)
- **show mpls forwarding-table labels local label**

Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

- **clear ip bgp mp-bgp neighbor soft in**
- **clear ip bgp mp-bgp neighbor soft out**

• CSCtn22728

Symptoms: See the following:

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ?
<cr>

Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on command:
    destination int g11/48
due to parser return error
```

Conditions: This symptom is seen when using an unsupported interface CLI option with the **destination** keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

Workaround: Do not issue not applicable commands.

• CSCtn26785

Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

```
3845#sh int atm 1/0 stat
ATM1/0
Switching path      Pkts In      Chars In      Pkts Out      Chars Out
Processor           98170        10995040      1              68
Route cache         0            0              98170         10995040
Total               98170        10995040      98171         10995108
3845#
```

```
3845#sh cef int atm 1/0
ATM1/0 is up (if_number 5)
  Corresponding hwidb fast_if_number 5
  Corresponding hwidb firstsw->if_number 5
  Internet address is 64.65.248.174/30
  ICMP redirects are never sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Input features: Ingress-NetFlow
  Output features: Post-Ingress-NetFlow
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is ATM1/0
  Fast switching type 9, interface type 138
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
```

```

Input fast flags 0x0, Output fast flags 0x0
ifindex 5(5)
Slot Slot unit 0 VC -1
IP MTU 4470
3845#

```

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn27599

Symptoms: The OIR of NM-1T3/E3 line card crashes the router.

Conditions: This symptom is observed only on the Cisco 3945 router.

Workaround: There is no workaround.

- CSCtn38996

Symptoms: All MVPN traffic is getting blackholed when peer is reachable using a TE Tunnel, and an interface flap is done so that secondary path can be selected. The multicast route does not contain a native path using the physical interface.

Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn48744

Symptoms: Memory leaks on OER border router while running PfR-IPSLA configuration.

Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

Workaround: There is no workaround.

- CSCtn53094

Symptoms: The router crashes or generates the following error:

```

%SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process=
"Mwheel Process", ipl= 2, pid= 315

```

Conditions: This symptom is observed when toggling very fast between the **ip pim mode** and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

Workaround: Avoid fast toggling of the **pim mode** command if possible when it is only present on a single interface.

- CSCtn72939

Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.

Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.

Workaround: Configure bridge-group under that xconnect interface.

- CSCtn76183

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

- CSCtn77154

Symptoms: The Stateful Inspection Feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets being punted to the CPU. This causes overall performance degradation.

Conditions: This symptom is observed when two outside NAT interfaces are configured and “no ip nat service nbar” is configured on the interface.

Workaround: Configure “ip nbar protocol discovery” on the interface.

- CSCtn87012

Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

Workaround: Pick up the phone during the ringing OFF cycle.

- CSCtn93891

Symptoms: Multicast traffic is getting blocked.

Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

Workaround: There is no workaround.

- CSCtn96521

Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast peer** command on the router.

Conditions: This symptom occurs with the following conditions:

Router3 ---ebgp--- Router1 ---ibgp--- Router2

```
ROUTER1:
-----
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
!

router ospf 100
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.3 remote-as 11
```

```

!
ROUTER2:
-----
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip pim sparse-mode
!
router ospf 100
  redistribute static
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

ROUTER3:
-----
interface Ethernet0/0
  ip address 10.1.1.3 255.255.255.0
  ip pim sparse-mode
!
router bgp 11
  bgp log-neighbor-changes
  network 0.0.0.0
  network 0.0.0.0 mask 255.255.255.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCto00796

Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)

Workaround: Soft clear the peer that missed getting the RT.

- CSCto02448

Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

Conditions: This symptom is observed with the following conditions:

1. The neighbor is configured with soft-reconfiguration inbound.
2. The inbound routemap is not configured for the neighbor.
3. The non-routemap inbound policy (filter-list) allows the path.

Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto03446

Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

Conditions: This symptom occurs with a flat policy attached to the frame-relay interface with traffic shaping enabled.

Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto07586

Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

Conditions: This symptom occurs with the following conditions:

1. Create an IOS image that does not IPV6 enabled.
2. Enable BFD on an interface.
3. Configure an IPV4 static route with BFD routing through the above interface.

The IPV4 BFD session does not get established, so the static route does not get installed.

Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

- Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
- ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>

- CSCto08754

Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.

Conditions: This symptom occurs when the crypto VTI interface becomes wedged.

Workaround: There is no workaround.

- CSCto11238

Symptoms: OSPF cannot be enabled on a tunnel interface by using either the network statement under OSPF or by enabling OSPF directly under the interface.

```
Router#show ip osp neighbor tunXXX
%OSPF: OSPF not enabled on TunnelXXX
```

Conditions: This symptom is observed in both Cisco IOS Release 15.1S and Cisco IOS Release 15.1T IOS software trains. The problem is triggered by configuring either WCCP, L3VPN, or mGRE. A tunnel configured with any of these will have dynamic routing disabled on it. If this is then deleted, the idb is reused by a new tunnel created via the CLI. This newly created tunnel will still have dynamic routing disabled on it and therefore ospf cannot run on it.

Workaround: Once the problem has occurred, the only way to recover is to reload the router. If WCCP, L3VPN, or mGRE are never configured, the issue will not be seen.

- CSCto13254

Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

```
Hash verification failed for file <temp location of profile>
```

Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

Workaround: Remove the profile from the Cisco IOS headend.

- CSCto14435

Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto15361

Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16597

Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.

Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.

Workaround: There is no workaround.

- CSCto24338

Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0xFFFFFFFF
```

Conditions: This symptom occurs with NAT+SIP.

Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

- CSCto31265

Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

Workaround 1: Delete/readd the static route that generates Type7.

Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto41165

Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit | deny** command, and then the **no ip extcommunity-list 55 permit | deny** command.

Conditions: This symptom occurs when the standby router is configured.

Workaround: There is no workaround.

- CSCto44581

Symptoms: The router crashes on high call volume.

Conditions: This symptom occurs on high call volume.

Workaround: There is no workaround.

- CSCto46716

Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto47524

Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.

A **show process memory sorted** command may initially show “MallocLite” growing. By disabling mallocite with the following:

```
config t
no memory lite
end
```

one may start to see process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80mb per day.

Conditions: This symptom is observed on a Cisco ASR 1002 router.

Workaround: Disable IP SLA on the affected router, if possible.

- CSCto50255

Symptoms: Memory leak occurs while running UDP echo operation.

Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory pid** command.

Workaround: There is no workaround.

- CSCto53332

Symptoms: A router configured for IPSEC accounting may display the following error message:

```
%AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
```

This does not seem to result in any impact apart from intermittently lost accounting messages.

Conditions: This symptom occurs when ipsec accounting is active.

Workaround: There is no workaround.

- CSCto63954

Symptoms: A router with GETVPN configurations is continuously crashing.

Conditions: This symptom is seen with GETVPN related configurations with the fail-close feature activated.

Workaround: There is no workaround.

- CSCto68554

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfb>

- CSCto81814

Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

Conditions: This symptom is only observed when ECDSA certificates are used for IKEv2, and not with RSA certs or with IKEv1.

Workaround: There is no workaround.

- CSCto86833

Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DN's with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes a significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

Workaround: If possible, reduce the number of voice ports automatically generated by the number DNs and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- CSCto88686

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCtq05636

Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg.

For example:

```
Received: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
Sent: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
```

In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq09899

Symptoms: The VXML gateway crashes.

Conditions: This symptom occurs during the load test, when the **show mrcp client session active** is used.

Workaround: There is no workaround.

- CSCtq10684

Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

Conditions: This symptom occurs when tunnel flap is observed before the crash.

Workaround: A possible workaround is to reload the box.

- CSCtq15247

Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

For example:

```
LAC1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LAC1(config)#interface virtual-ppp1
LAC1(config-if)#no pseudowire
LAC1(config-if)#exit
LAC1(config)#no interface virtual-ppp1
```

- CSCtq27180

Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.

Conditions: This symptom is observed only on IOS internal releases.

Workaround: There is no workaround.

Further Problem Description: The following LOG messages and errors are found:

```
Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed
-Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z
63765DC8z
Mar 30 01:27:38.447: %LICENSE-2-VLS_ERROR: 'VLSsetInstallLicenseStorage'
failed with an error - rc = 136 - 'Error[136]: Specified license store
doesn't exists.'
-Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z
63765DE4z 63765DC8z
```

- CSCtq28732

Symptoms: Memory leak is observed when device is configured **parameter-map type inspectglobal**.

Conditions: Device is configured with **parameter-map type inspect global**.

See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>

Workaround: There is no workaround.

- CSCtq29554

Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

Workaround: Reload the failing line card to recover it.

- CSCtq30875

Symptoms: A Cisco ISR G1 will display “March 11, 2011” when the **show clock** command is entered. This will effect the functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

Workaround: The clock can be set manually via CLI.

- CSCtq36726

Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual-access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

Workaround: Reconfigure the Virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

- CSCtq39406

Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

Conditions: This symptom occurs when you set up an energywise domain via the CLI, and then set the energywise level to zero on a SM or ISM.

Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- CSCtq49408

Symptoms: Analog phone calls (fxs) cannot be made with CME/SCCP.

Conditions: This symptom occurs when SCCP support for FXS is missing in IAD2435.

Workaround: There is no workaround.

- CSCtq61850

Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

Workaround: There is no workaround.

- CSCtq64951

Symptoms: The following message is displayed:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto
functionality with securityk9 technology package license.
```

The **show platform cerm** command output shows all tunnels in use by SSLVPN.

```
Number of tunnels      225
...
SSLVPN D D              225      N/A
```

The **show webvpn session context all** command output shows no or very few active sessions.

```
WebVPN context name: SSL_Context
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
```

Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq91176

Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtl22737

Symptoms: The config replace feature fails to remove “hold-queue” interface subcommands.

Conditions: This symptom occurs when the config replace feature fails to remove “hold-queue” interface subcommands.

Workaround: Manually remove the “hold-queue” configuration. With this fix, the behavior has changed for the “no” form of this command.

In short,

```
no hold-queue <any random value(not necessarily the same configured value)>
out [for out queue]
```

```
no hold-queue <any random value(not necessarily the same configured value)>
in [for in queue]
```

Resolved Caveats—Cisco IOS Release 15.1(2)T3

Cisco IOS Release 15.1(2)T3 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T3 but may be open in previous Cisco IOS releases.

- CSCso02147

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>

- CSCtd10712

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)

- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>

- CSCtd90030

Symptoms: A Cisco 2851 router may crash with a bus error.

Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd91542

Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

Conditions: The symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

Workaround: Avoid using the **show ip multicast rpf tracked** command.

Further Problem Description: The command **show ip multicast rpf tracked** is not intended for customer use and is being deprecated.

- CSCte01606

Symptoms: When Bidirectional Forward Detection (BFD) is enabled, issuing certain CLI commands that are not preemption safe may cause the device to restart. This condition has been seen when issuing commands such as “show mem” or “show mem frag detail”.

Conditions: The issue may occur if BFD is enabled on a device that utilizes Pseudo Preemption to implement this feature. The device must be running an affected software build.

Workaround: Disable BFD.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.4/3.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C>

CVE ID CVE-2010-3049 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtf36402

Symptoms: A Cisco router crashes when the user telnets and Transmission Control Block is cleared for that session before entering the password.

Conditions: This symptom is observed when aaa authentication protocol is set to TACACS.

Workaround: Do not clear the Transmission Control Block for a session before entering the password.

- CSCtf54561

Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf vrf-name** command is issued.

Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

Workaround: Command should not be issued when many topology changes occur on interface flaps.

- CSCtf56107

Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

Conditions: The symptom is observed when an unknown notify message is received.

Workaround: There is no workaround.

- CSCtf72328

Symptoms: BFD IPv4 Static does not fully support AdminDown.

Conditions: The symptom is observed with the following setup and configuration:

```
Router 1:
interface e0/0
ip address 192.168.1.1 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.10.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.2
ip route 10.20.0.0 255.255.0.0 e0/0 192.168.1.2

Router 2:
interface e0/0
ip address 192.168.1.2 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.20.1.1 255.255.0.0
exit

ip route static bfd e0/0 192.168.1.1
ip route 10.10.0.0 255.255.0.0 e0/0 192.168.1.1

interface e0/0
no ip route static bfd e0/0 192.168.1.1
```

Though the BFD state is DOWN the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtg31210

Symptoms: A router may reload.

Conditions: The symptom is observed when using the PfR feature to control path selection with EIGRP and when **debug oer border routes eigrp detail** is enabled.

Workaround: Do not configure debugs **debug oer border routes eigrp** or **debug oer border routes eigrp detail**.

Further Problem Description: The issue is not seen in Cisco IOS Release 15.0 (1)M4.

- CSCtg42279

Symptoms: A Cisco label switch router (LSR) crashes when an MPLS traceroute is issued.

Conditions: This symptom is observed when executing MPLS traceroute over a IPsec-protected GRE tunnel.

Workaround: There is no workaround.

- CSCtg63096

Symptoms: The **deny ip any any fragments** command shows a high number of hits for traffic that may not be truly fragmented.

Conditions: This symptom occurs when “deny ip any any fragments” may be configured at the top of the ACL.

Workaround: There is no workaround.

- CSCtg64175

Symptoms: The ISIS route is missing the P2P link, it is mistakenly marked as “parallel p2p adjacency suppressed”.

Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial ITH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCtg67346

Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show “Di1 DDR: dialer_fsm_pending() di1”.

Conditions: The conditions are unknown at this time.

Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCtg73631

Symptoms: Spurious access or crash.

Conditions: EIGRP undergoes a route delete event for a route that is both redistributed and learned as an external. The redistributed route is deleted and external route promoted. An error in the route deletion codepath may result in spurious access or crash.

Workaround: There is no workaround.

Further Problem Description: Issue is not present in Cisco IOS Release 15.0(1) M4.

- CSCth01394

Symptoms: On a Cisco 7606 router that is running Cisco IOS Release 12.2(33) SRD3 with SIP200/SPA-4XCT3/DS0, when you have ppp multilink interface(s) configured with member links from same SPA (software based multilink) and you physically remove SPA, you will see that upon executing the **show ppp multilink** command, the multilink interface still has reference for member links. If you do the **sh run int serialx/y** command, you will get message interface not found.

Conditions: This issue is consistently reproducible.

Workaround: There is no workaround.

- CSCth05778

Symptoms: Router is showing memory leaks.

Conditions: The symptom is observed when the remote end is sending LCP conf_req messages to a Cisco 10000 series router a lot frequently (1 per 4 msec) than the normal scenario (1 per 2 seconds).

Workaround: Shut down the PPP link that is flapping.

- CSCth06812

Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:

```
R1(config)#parser view SUPPORT
R1(config-view)# secret cisco
R1(config-view)# commands exec include ping
R1(config-view)# commands exec include configure terminal
R1(config-view)# commands exec include show ip ospf neighbor      <--Where
we see the hang
```

Workaround: Do not configure “commands exec include show ip ospf neighbor” command in parser view configuration.

- CSCth14305

Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if linkmembers flap as the changes in bandwidth will not be handled correctly.

Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth20696

Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

Conditions: The symptom is observed with Cisco IOS Release 12.4(25c).

Workaround: There is no workaround.

- CSCth37580

Symptoms: Dampening route is present even after removing “bgp dampening”.

Conditions: The symptom is observed under the following conditions:

- DUT connects to RTRA with eBGP + VPNv4.
- eBGP + VPNv4 peer session is established and DUT.
- Also DUT has VRF (same RD) as route advertised by RTRA.

In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

Workaround: There is no workaround.

- CSCth59784

Symptoms: Process watchdog timeout crashinfo file not written into flash for Cisco 887 router.

Conditions: The symptom is observed on a Cisco 887 router.

- Workaround: There is no workaround.
- CSCth84233

Symptoms: Router may crash due to Redzone memory block corruption (I/O) when “qos pre-classify” is configured under tunnel interfaces. The packet is overwriting the next block.

Conditions: The trigger for this issue is configuring “qos pre-classify”.

Workaround: Remove “qos pre-classify”.
 - CSCth93218

Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

Workaround: There is no workaround.
 - CSCth94814

Symptoms: Crash is seen in static route component.

Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.

Workaround: There is no workaround.
 - CSCth94827

Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima- group on a SONET-ACR controller.

Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

Workaround: There is no workaround.
 - CSCti01971

Symptoms: The active router crashes during a switchover in a scaled BFD IPv6 setup.

Conditions: The router is configured with a larger number of IPv6 routes with BFD sessions configured. (The test was done with 500 BFD IPv6 sessions.)

Workaround: There is no workaround.
 - CSCti03261

Symptoms: A Cisco router may crash due to a WATCHDOG timeout.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M3 and when attempting to remove a line from a Named Access List that is being used by a QoS service policy.

Workaround: There is no workaround.
 - CSCti04754

Symptoms: PPPoE sessions are stuck at attempting state forever.

Conditions: This symptom is seen when sessions are triggered during SSO time, which get stuck at attempting state.

Workaround: Clear attempting state sessions by the **clear** command from box.
 - CSCti05663

Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

Conditions: The symptom is observed in the case of an numbered relay.

Workaround: There is no workaround.

- CSCti10518

Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

Workaround: There is no workaround.

- CSCti17841

Symptoms: Removing “match condition” from a class map crashes the router.

Conditions: The symptom is observed when you remove “match condition” from a class map.

Workaround: There is no workaround.

- CSCti22091

Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

Conditions: The symptom is observed when PfR is configured with the following conditions:

1. list > application > filter > prefix-list
2. Learn > traffic-class: keys
3. Learn > traffic-class: filter > ACL

Workaround: There is no workaround.

- CSCti24577

Symptoms: System crashes on active or hangs on standby.

Conditions: The symptom is observed when a banner command is in the configuration.

Workaround: Remove all banner commands.

- CSCti25339

Symptoms: Cisco IOS device may experience a device reload.

Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2010-3050 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti25780

Symptoms: One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

Conditions: This symptom is observed when some of the files are compiled with optimization.

Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- CSCti34396

Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

Conditions: The symptom is seen when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
  set ip next-hop <router ip address>
!
router bgp <asn>
  address-family ipv4 vrf <vrf name>
  redistribute static route-map static-nexthop-rewrite
  exit-address-family
exit
exit
```

Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

For example, if you had: ip route x.x.x.x 255.255.255.0 y.y.y.y And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with: ip route x.x.x.x 255.255.255.0 interface serial2/0

Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration “set ip next-hop self” is added to route-maps.

When used in conjunction with the newly added configuration:

```
router bgp <asn>
  address-family vpnv4 unicast
    bgp route-map priority
```

The “set ip next-hop self” will override “next-hop unchanged allpaths” for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti36393

Symptoms: Spurious memory access messages and tracebacks appear on console after disabling and re-enabling WAAS on an interface.

Conditions: The symptom is observed when open flows are on the router while the configuration commands are given.

Workaround: There is no workaround.

- CSCti50607

Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

Workaround: There is no workaround.

- CSCti51145

Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

Conditions: In order to see this problem, ALL of the following conditions must be met:

- The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword **established** or **eq bgp**.
- It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
- When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
- Both peers must be multisession capable.
- “transport multi-session” must not be configured on either device, or enabled by default on either device.
- “graceful restart” must not be configured.

Workarounds:

1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the 12.2(33)SB router is the one not reloading.

- CSCti61949

Symptoms: Unexpected reload with a “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti66076

Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

Condition: This symptom is observed under the following conditions:

- HSRP version 1 is the protocol that must be used.
- Use HSRP with sub-interfaces on ES20 module *Reload the ES20 module

Workaround: Change to HSRPv2, which is not exposed to the issue.

Alternate Workarounds:

1. econfigure HSRP on all subinterfaces
2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti67102

Symptoms: Tunnel disables due to recursive routing loop in RIB.

Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

Workaround: There is no workaround.

- CSCti67447

Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

Conditions: The symptom is observed under the following conditions:

1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2.
2. Enable MPLS LDP GR.

Workaround: There is no workaround.

- CSCti67905

Symptoms: A Cisco router may experience a crash.

Conditions: This has been experienced on Cisco routers running Cisco IOS Release 15.1(2)T and Release 15.1(2)T1. The routers are configured with IOS firewall and are inspecting FTP packets.

Workaround: There is no workaround.

- CSCti68721

Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

Workaround: If the symptom occurs, repeat the command.

- CSCti75666

Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.

Workaround: Convert H.323 leg to SIP.

- CSCti79848

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>

- CSCti84762

Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

Conditions: This is seen with peer flaps or route churn and with an interface flap.

Workaround: Do a hard reset of the stuck peers.

- CSCti85446

Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

Conditions: The symptom is observed with the following conditions:

1. Configure a nexthop static route with permanent keyword.
2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
3. Change the configuration in such a way that nexthop is reachable.
4. Configure a new static route through the same nexthop IP address used in step 1.

Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti87502

Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.

Conditions: This symptom is observed when attempting to launch CP Express.

Workaround: A power cycle fixes the issue temporarily.

- CSCti91036

Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Release 15.1(2)T.

Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti98219

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>

- CSCtj00039

Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj05198

Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

Conditions: This symptom is observed when there are two EIGRP router processes.

Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07904

Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

Conditions: The symptom is observed when “no passive interface” is configured.

Workaround: Do not configure “passive-interface default” and allow the interface to be non-passive by default. Configure “passive-interface *interface*” for the interface to be passive.

- CSCtj17545

Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

template peer-session ce-v4 transport connection-mode passive

- CSCtj20163

Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

Conditions: The symptom is observed with the following conditions:

1. Execute **show mpls mldp database**.

2. Reload Encap PE.
3. Crash seen on P router when MLDP neighbors go down.

Workaround: There is no workaround.

- CSCtj21045

Symptoms: Header compression decodes RTP timestamp incorrectly.

Conditions: This issue occurs mainly with IPHC format compression interacting with older Cisco IOS releases.

Workaround: Use IETF format compression.

- CSCtj21696

Symptoms: The virtual access interface remains down/down after an upgrade and reload.

Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv
NAME: "chassis", DESCR: "2801 chassis" PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet" PID: CISCO2801 ,
VID: V04 , SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard" PID:
VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch" PID: HWIC-4ESW , VID: V01 , SN:
FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire" PID:
WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capacity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB
```

Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

Symptoms: The following traceback is observed when **clear ip bgp *** is done:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data
5905A0A8 chunkmagic 120000 chunk_freemagic 4B310CC0
-Process= "BGP Scanner", ipl= 0, pid= 549
with call stack
0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
0x403A4E84:bgp_scanner(0x403a4c50)+0x234
```

Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

```
Router# show ip bgp sum
BGP router identifier 10.0.0.1, local AS number 65000
BGP table version is 1228001, main routing table version 1228001 604000
network entries using 106304000 bytes of memory
604000 path entries using 31408000 bytes of memory
762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

The **clear ip bgp *** command is not a very common operation in production network.

Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj27251

Symptoms: A router may crash when modifying a QoS class-map.

Conditions: The symptom is observed when modifying a QoS class-map which is being referenced by two or more policy-maps while traffic is matching the class-map and traversing the router.

Workaround: Remove the policy-maps that match the class-map to be modified by issuing **no service-policy input/output *policy-map name***, make changes to the class-map, then re-apply the policy-maps by issuing **service-policy input/output *policy-map name***.

- CSCtj28747

Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj32574

Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

```
router eigrp 1
 redistribute connected
no redistribute connected
```

The **no redistribute connected** command is not being backed up to the standby.

Conditions: The symptom is observed with any redistribute-related commands.

Workaround: There is no workaround.

- CSCtj39558

Symptoms: Sub-interface queue depth cannot be configured.

Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

Workaround: There is no workaround.

- CSCtj39664

Symptoms: A router that is running Cisco IOS Release 15.1(2)T1 may crash when attempting to configure Zone-Based Firewall.

Conditions: The symptoms are observed when attempting to configure zone-pair. It occurs only with a Cisco 861 router.

Workaround: There is no workaround.

- CSCtj41016

Symptoms: The assertion failures below will appear on the console continuously in Cisco 888E platform and the router prompt will not do any configurations:

```
ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
ASSERTION FAILED: file "../src-m8300-c880/c880_shdsl_efm_io.c", line 653
```

Conditions: The symptom is observed on Cisco 888E routers.

Workaround: There is no workaround.

- CSCtj41194

Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6>

- CSCtj47736

Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

Workaround: There is no workaround.

- CSCtj48629

Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtj52077

Symptoms: Policy at subinterface is not accepted with CBWFQ.

Conditions: This symptom is observed when policy is used in Ethernet subinterface.

Workaround: There is no workaround.

- CSCtj53363

Symptoms: Router hangs and console does not respond indefinitely.

Conditions: The symptom is observed with the following conditions:

- AIM-VPN in ISR + ZBFW; or
- A Cisco 2811/2821 Onboard VPN + ZBFW.
- Once traffic starts, router hangs within minutes.

Workaround 1: If running a Cisco 2811/2821, use sw crypto + ZBFW.

Workaround 2: If running with a Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj58943

Symptoms: Standby RP reloads due to line by line sync failure for **encapsulation dot1q 1381** command:

```
Config Sync: Line-by-Line sync verifying failure on command: encap dot1Q 1381 due to
parser return error
rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync, Reason:
Configuration mismatch
```

Conditions: Symptom occurs when issuing a configuration command under a sub-interface mode.

Workaround: There is no workaround.

- CSCtj65553

Symptoms: Static route that is installed in default table is missing.

Conditions: Static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on Cisco Catalyst 3000 series switching module.

Workaround: Configure the missing static route.

- CSCtj66235

Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

```
%SYS-6-STACKLOW: Stack for process voice file acct dump running low, 0/6000
```

Conditions: The crash suggests that the issue is just one of inefficient stack usage.

Workaround: There is no workaround.

- CSCtj69577

Symptoms: When congestion occurs on a QoS-enabled output interface, output rate significantly decreases.

Conditions: The symptoms are observed under the following conditions:

1. 3945E outbound interface is connected to 100M link.
2. QoS (LLQ/Fair Queue) is configured on 3945E outbound interface.
3. Congestion occurs on outbound interface.

Workaround: Reload the router.

Further Problem Description: This issue is resolved after a reload but the shutdown/no shutdown commands can cause the same issue.

- CSCtj69886

Symptoms: NTP multicast over multiple hops.

Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

Workaround: There is no workaround.

- CSCtj77004

Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

Conditions: The symptom is observed when “archive log config” is configured.

Workaround: There is no workaround.

- CSCtj77477

Symptom: High delay in priority queue when using CBWFQ/LLQ.

For example: EFM rate 2304 kbps

888E Average delay: 42ms

888E Max delay: 63ms

HWIC-4SHDSL-E Average delay: 216ms

HWIC-4SHDSL-E Max delay: 361ms

Conditions: The symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface.

For example: EFM rate 2304 kbps

```
policy-map CHILD
  class voice
    priority percent 25
  class business
    bandwidth percent 50
policy-map PARENT
  class class-default
    shape average 2100000 8400 0
  service-policy CHILD
```

- CSCtj77819

Symptoms: When dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration), then it is not effective. It is not resetting the idle timeout when outgoing interesting traffic is seen.

Conditions: The symptom is observed when dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration).

Workaround: Reconfigure “dialer idle-timeout” with any value (even default of 120 secs).

- CSCtj77963

Symptoms: Resets are observed on low speed links.

Conditions: The symptom is observed on low speed interfaces over the WAN that produce retransmissions, out of order segments, etc.

Workaround: There is no workaround.

- CSCtj78210

Symptoms: One-way audio. Moves from one port to another when the router is rebooted.

Conditions: The symptom is observed when using multiple “session protocol multicast”, “connection trunk” configurations for LMR, E&M Immediate, and/or other multicast applications, such as the conditions where this was first detected, in a Radio over IP solution. Only affects PVDM3.

Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

For example, configure:

```
voice-card 0 (1... 2... etc...)
dspfarm
dsp service dspfarm

dspfarm profile x conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x2 conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown
```



```

dspfarm profile x3 conf
max sessions xx << use maximum (if allowed)
max partic << use the maximum (if allowed)
associate app sccp
no shutdown

dspfarm profile x conf
shutdown
no dspfarm profile x conf

```

The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- CSCtj81533

Symptoms: The following error messages is seen:

```
np_vsmgr_modify_connection: invalid service id 11 passed
```

No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

Workaround: There is no workaround.

- CSCtj82292

Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

Conditions: This issue occurs when summary address is advertised as follows:

```
ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
```

Workaround: There is no workaround.

- CSCtj84901

Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

1. Service Ready Engine modules (ISM and SM SRE)
2. Etherswitch modules (SM and EHWIC)

If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj87180

Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9):

Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

Workaround: There is no workaround.

- CSCtj89941

Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

Conditions: Testbed setup:

1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured.
2. Use IXIA to generate 1Gbps traffic.
3. Wait until all the SAs have been established and traffic is stable.
4. Use CLI **clear crypto session** on EzVPN simulator.

Workaround: There is no workaround.

- CSCtj90342

Symptoms: A Cisco HWIC-2T module installed on a Cisco 2901, 2911 or 2921 router configured with “physical-layer async” (Async mode) delays printing the characters that you type in the terminal window.

Conditions: This symptom is observed on Cisco 2901, 2911, and 2921 platforms with Cisco HWIC-2T modules installed and running any Cisco IOS 15.X release.

This symptom is not observed on a Cisco 2951 platform.

Workaround: There is no workaround.

Further Problem Description: In a production environment, the first data string may not be transmitted until you enter the second string. For example, reverse telnet to the line using the command prompt of PC. A blank screen is opened where you will type. Now, using hyperterminal software, connect HWIC- 2T to your PC (similar to the console connection). You will see a blank screen on the software. Start typing numbers such as 1,2,3,4, and 5 at the command prompt. “2” will not be displayed until you press “3” at the command prompt, “4” will not show up until you press “5,” and so forth.

- CSCtj91764

Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

Conditions: The crash happens during a complete SNMP MIB walk.

Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj94617

Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

Conditions: This symptom is observed when issuing the **show running** command.

Workaround: There is no workaround.

Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

- CSCtj96915

Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

Conditions: Unknown. See Further Problem Description below.

Workaround: There is no workaround. Only power cycle can remove the symptom.

Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtk02647

Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

Workaround: There is no workaround.

- CSCtk06548

Symptoms: Using CCBU CVP solution, SIP calls are disconnected during stress test.

Conditions: The symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by SIP stack. It is seen with PI14 image testing.

Workaround: Use PI12 image.

Further Problem Description: The fundamental issue involves the selective ack (SACK) feature. An alternative workaround would be to disable the “SACK Permitted” option from the peer.

- CSCtk12608

Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T and 15.1(01)S and with the following configurations:

Router 1:

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!

router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.0.1 remote-as 200
 neighbor 172.16.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 10.10.200.1
ip route 172.16.0.1 255.255.255.255 10.0.12.2
ip route 172.16.0.1 255.255.255.255 10.0.120.2
```

Router 2:

```

interface Loopback200
 ip address 10.10.200.1 255.255.255.0
!
interface Loopback201
 ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.10.200.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!

```

Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12681

Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk35953

Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

Conditions: The symptom is observed only if DUT has eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from VPNv4 peer.

Workaround: A hard reset of the session will remove the dampening information.

- CSCtk52599

Symptoms: A Cisco 888E router does not train up with a third-party vendor’s DSLAM.

Conditions: The symptom is observed when the DSLAM is running the new firmware.

Workaround: There is no workaround.

- CSCtk53130

Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

```
Incompatible with ipv6 command on Vp1 - command rejected.
```

Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

Workaround: There is no workaround.

- CSCtk53534
Symptoms: Router crashes.
Conditions: The symptom is observed with some combination of zone-based firewall and policy configuration and with IPv6 traffic.
Workaround: Disable global parameter-map.
- CSCtk56570
Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.
Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.
Workaround: Disable media transcoder-high-density.
- CSCtk56817
Symptoms: Router crashes.
Conditions: The symptom is observed when pinging the dialer interface attached to the ATM interface.
Workaround: There is no workaround.
- CSCtk62247
Symptoms: IKEv2 session fails to come up with RSA sign authentication.
Conditions: The symptom is observed with a hierarchical CA server structure.
Workaround: Use non-hierarchical CA servers.
- CSCtk66979
Symptoms: Hold queue on an ATM interface does not work.
Conditions: This symptom is observed when hold-queue per VC is configured on ATM interfaces (NM-1A-T3/E3) on ISR G2.
Workaround: There is no direct workaround. It will work only for default hold-queue size or maximum hold queue size under an ATM interface.
- CSCtk67709
Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

```
ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432-k9.pkg
SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
```


Conditions: This symptom is observed with AnyConnect 3.0.
Workaround: There is no workaround.
- CSCtk74970
Symptoms: TE autoroute announced tunnel is not installed in the routing table.
Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute announced tunnel is not installed in the routing table.
Workaround: Configure “no ip routing protocol purge interface”.

- CSCtk84116

Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

Workaround: There is no workaround.

- CSCtk95992

Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

Workaround: Configure the command **dls w udp-disable**.

Further Problem Description: This symptom occurs in the following (and later) Cisco IOS releases:

- 12.4(15)T14
- 12.4(24)T4
- 15.0(1)M3
- 15.1(1)S
- 15.1(2)T
- 12.2(33)SXI4
- 12.2(33)SXI4a

- CSCtl04285

Symptoms: After a BGP flap or provisioning a new session, the BGP route reflector will not advertise new IPv4 MDT routes to PEs.

Conditions: This symptom is observed with BGP session flap or when provisioning a new session.

Workaround: Enter the **clear ip bgp *** command.

- CSCtl08014

Symptoms: Router crashes with memory corruption symptoms.

Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

Workaround: There is no workaround.

- CSCtl21695

Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million. Debug vpdn l2x ev/er shows:

```
PPTP      ____:_____: TCP connect reqd from 0.0.0.0:49257
PPTP      ____:_____: PPTP, no cc in l2x
```

Conditions: This symptom occurs when LNS is configured for PPTP aggregation and over one millions tunnels have been accepted (on VPDN level).

Workaround: Reload LNS.

- CSCtl21884

Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent even though the static route goes down.

Conditions: The symptom is observed under the following conditions:

- Enable auto-summary under the BGP process.

- Static route is brought into the BGP table via the **network** command.

Workaround: Use **clear ip bgp *** or disable “auto-summary” under the BGP process.

- CSCtl47666

Symptom: Intermittent call drops for CME SNR calls that go to voicemail.

Conditions: This symptom is observed on a Cisco IP phone with SNR configured. When the “no answer” timer is reached, the call will intermittently drop instead of going to voicemail.

Workaround: There is no workaround.

- CSCtl50815

Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

```
%OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
Non-OER, OOP Reason <reason>
```

Conditions: The symptom is observed under the following conditions:

- Use ECMP.
- Use **mode monitor passive**.

Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl57055

Symptoms: A router may unexpectedly reload when the rttMonStatsTotalsEntry MIB is polled by SNMP.

Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release, is configured for SNMP polling, and when the rttMonStatsTotalsEntry is polled with an IP SLA probe configured.

Workaround 1: Configure NMS to stop polling the rttMonStatsTotalsEntry or create a view and block the MIB on the router.

Workaround 2: The issue only affects Cisco IOS 15.1T releases, so use a Cisco IOS 15.0(1)M rebuild or earlier.

- CSCtl67195

Symptoms: The following three BGP debug commands are not allowed to enable:

```
debug ip bgp vpnv4 unicast
debug ip bgp vpnv6 unicast
debug ip bgp ipv6 unicast
```

Conditions: The symptom is observed with the above BGP debug commands.

Workaround: There is no workaround.

- CSCtl73914

Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

Conditions: The symptom is observed if the P-Associated-URI of the 200 Ok response contains any special characters (!*.) in Tel URI Parsing.

Workaround: There is no workaround.

- CSCtl77735

Symptoms: Saving a configuration to NVRAM may fail.

Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

Workaround: Erasing the startup configuration and saving again may recover the configuration.

- CSCtl87879

Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

Workaround: There is no workaround.

- CSCtl88066

Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

Conditions: The symptom is observed when BGP is configured and you issue one of the following commands:

show ip bgp all attr nexthop

show ip bgp all attr nexthop rib-filter

Workaround: Do not issue either of these commands with the "all" keyword. Instead, issue the address-family specific version of the command for the address family you are interested in.

For example, the following are safe:

show ip bgp ipv4 unicast attr nexthop

show ip bgp attr nexthop

show ip bgp vpnv4 vrf *vrfname* attr nexthop

Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing, and where this fix is not integrated are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl92014

Symptoms: After a reprompt element, "enumerate", using internal variables like `_prompt` or `_dmf`, no longer produces a valid list of options and repeats the last option.

Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T and later releases.

Workaround: There is no workaround.

- CSCtl98270
Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.
Conditions: The symptom is observed in Cisco IOS 15.1(2)T2 Release and later releases.
Workaround: Execute a shut/no shut to fix the issue.
- CSCtn01832
Symptoms: The following command sequence crashes the router at check syntax mode:
config check syntax route-map hello match local-preference no match local-preference
Conditions: The symptom is observed with the commands above.
Workaround: There is no workaround.
- CSCtn08613
Symptoms: Cisco router crashes when interfacing with UCCX.
Conditions: This has been experienced on a UC560 running Cisco IOS Release 15.1(2)T2 when making consult transfer calls.
Workaround: There is no workaround.
- CSCtn46263
Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.
Conditions: This symptom is observed during retransmissions and window throttling of requests.
Workaround: There is no workaround.
- CSCtn51740
Symptoms: Memory leak is seen in EzVPN process.
Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.
Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T2a

Cisco IOS Release 15.1(2)T2a is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T2a but may be open in previous Cisco IOS releases.

- CSCtj39558
Symptoms: Subinterface queue depth cannot be configured.
Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.
Workaround: There is no workaround.
- CSCtj52077
Symptoms: Policy at subinterface is not accepted with CBWFQ.
Conditions: This symptom is observed when policy is used in Ethernet subinterface.
Workaround: There is no workaround.

- CSCtj66235

Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

```
%SYS-6-STACKLOW: Stack for process voice file acct dump running low, 0/6000
```

Conditions: The crash suggests that the issue is just one of inefficient stack usage.

Workaround: There is no workaround.

- CSCtj94617

Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

Conditions: This symptom is observed when issuing the **show running** command.

Workaround: There is no workaround.

Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

Resolved Caveats—Cisco IOS Release 15.1(2)T2

Cisco IOS Release 15.1(2)T2 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T2 but may be open in previous Cisco IOS releases.

- CSCsu95339

Symptoms: Output from the **show idmgr session** command displays a corrupted service name.

Conditions: Enter the **show idmgr session** command.

Workaround: There is no workaround.

- CSCta53372

Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

Workaround: Reset the RRI session.

- CSCtb55576

Symptoms: When an HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic that is traversing the other interfaces is delayed for approximately 160 to 250 ms during the %LINK-3-UPDOWN event.

Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for approximately 160 to 250 ms.

Workaround: There is no workaround.

- CSCtc33679

Symptoms: Routes are not being controlled properly when PIRO is used.

Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

Workaround: There is no workaround.

- CSCtc55897

Symptoms: R2 will not advertise the routes.

Conditions: The symptom is observed under the following conditions:

1. R2 has two IBDG neighbors in the same update-group one neighbor with 4BAS and the other with 2BAS capability.
2. The locally originated routes or routes without any AS_PATH will not be advertised to this kind of group.

Workaround: Try to make the 2BAS and 4BAS neighbors fall into different update-groups by configuring dummy route-maps.

- CSCtd39579

Symptoms: A router crashes when we try to remove service-policy/waas from an interface.

Conditions: Traffic should be hitting the interface, CPU utilization should be high, and NAT should be applied on the interface as well.

Workaround:

1. Remove NAT from the interface.
2. Remove the service policy.
3. Re-apply NAT.

- CSCte20187

Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (1)
```

The label advertised may be different but it is always a reserved label (0- 15).

Additionally, the local PE will see No Label as the Outgoing Label in the MPLS forwarding table.

Conditions: This symptom is observed when bgp next-hop is configured under an interface.

Workaround: There is no workaround.

- CSCte61495

Symptoms: The following messages are seen with tracebacks:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process = Exec. %SYS-2-INTSCHED: 'suspend' at level 3 -Process= "Exec", ipl= 3, pid= 128,
```

Conditions: The symptom is observed when a large ACL is configured for the service policy. This happens only under ATM subinterfaces.

Workaround: Use small-sized ACLs for the service-policy.

- CSCte91259

Symptoms: A Cisco router may unexpectedly reload due to a bus error after displaying an “%IDMGR-3-INVALID_ID” error.

Conditions: The crash will be seen only if the router is using DHCP Client Dynamic DNS update.

Workaround: There is no workaround.

- CSCtg53953

Symptoms: A standby router reloads due to a parser sync issue when applying certain neighbor commands (neighbor <ip-address> disable-connected-check, neighbor <ip-address> peer-group pgrp, and others).

Conditions: This symptom applies only to situations where <ip-address> is the IP address of a peer that has a dynamically created session (a neighborhood that is the result of the “bgp listen range ...” feature).

Workaround: There is no workaround. Such a configuration should not be applied in the first place.

- CSCtg58786

Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

Workaround: There is no workaround.

- CSCtg59956

Symptoms: Active supervisor crashes when doing an SSO switchover.

Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

Workaround: There is no workaround.

- CSCtg60201

Symptoms: Unconfiguring the **maximum-path** command does not trigger a backup path calculation.

Conditions: This symptom is observed if addition-path install is configured along with the **maximum-path** command.

Workaround: Reconfigure “bgp additional-path install.”

- CSCtg84649

Symptoms: EIGRP is not forming adjacencies over virtual interfaces in a DVTI environment.

Conditions: This symptom is observed on a Cisco ASR 1000 platform with Cisco IOS Release 12.2(33)XNE or Release 12.2(33)XNF1.

Workaround: Remove the passive-interface configurations for Virtual-Template and then re-configure the passive-interface designation. For example,

```
Router# show run | b router
```

```
router eigrp 100
 network 10.1.0.0 0.0.31.255
 passive-interface default
 no passive-interface Virtual-Template1
```

```
Router(config)# router eigrp 100
Router(config-router)# no passive-interface default
Router(config-router)# passive-interface default
Router(config-router)# no passive Virtual-Template 1
```

- CSCtg94250

Symptoms: Removing **address-family ipv4 vrf <vrf>** (in router BGP) followed by **no ip vrf <vrf>** (where “vrf” is the same) could result in a crash.

Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

1. **no address-family ipv4 vrf <vrf>**

2. **no ip vrf <vrf>** 3. **ip vrf <vrf>**

The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).

2. Give sufficient time for (1) to complete before applying (2).

- CSCtg95940

Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

Workaround: There is no workaround.

Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCtg99114

Symptoms: The following error message with traceback is observed:

```
%IPC-5-REGPORTFAIL: Registering Control Port
```

Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.

Workaround: Drop IPC traffic using control-plane policing:

```
class-map match-all ipc
  match access-group name ipc
policy-map drop-ipc
  class ipc
    drop
ip access-list extended ipc
  permit udp any any eq 1975
control-plane
  service-policy input drop-ipc
```

- CSCth03022

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities.

Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCth11747

Symptoms: When a switchover occurs with GR enabled, sometimes the NSF states are not preserved and the forwarding entries are lost, leading to packet loss for a few seconds.

Conditions: This symptom is observed only with single sessions with GR configured when the restarting neighbor does a passive open. Chances of hitting this are low since this issue occurs because we receive a new open message before the old tcp session has a chance to reset.

Workaround: Configuring multi-session capability on the neighbor sessions or restricting the restarting neighbors connection to active mode would prevent this issue.

Further Problem Description: When an established session already exists between the GR-enabled routers, and the tcp has not yet notified of reset due to neighbor SSO, if the receiving router gets a new open from the restarting router, as per the RFC it is supposed to tear down the old session and accept the new connection. The old session was being torn down properly but it would take the service reset walker to completely free the session. In case of multi-sessions there was no problem in accepting the new session since multiple sessions are allowed. But in case of a single session that already exists, the new sessions are not allowed until the old session is completely freed. Hence, the new session was getting rejected and notification was sent to the restarting neighbor. The restarting neighbor, upon reception of this notification, would clear the NSF preserve bits and further opens would clear the NSF states on the receiving neighbor and hence the problem. The solution would be to accept the new connections in single session support neighbors when the GR reopen has marked the session for reset and de-linked the topologies. The topologies would be added to the new session and the connection accepted. The old session would be freed when service reset walker is invoked. So, for a transient period of time between the session mark reset and the session free, there would be multiple sessions established on the neighbor even though the neighbor was configured as single session. Dependent DDTs CSCtd99802 and CSCth90239 need to be committed along with this fix to ensure complete working of this functionality.

- CSCth13153

Symptoms: An incorrect UDLR Reporter exists on a router that is connected to a UDLR link and PIM-SM domain with auto-rp configurable.

Conditions: This symptom is observed on a Cisco 7200 series router with Cisco IOS Release 15.1(1.16)T0.1.

Workaround: There is no workaround.

- CSCth15105

Symptoms: BFD sessions flap after unplanned SSO (test crash).

Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

Workaround: There is no workaround.

- CSCth16011

Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

Conditions: Introduce loss to network.

Workaround: There is no workaround.

- CSCth18146

Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

Workaround: There is no workaround.

- CSCth25634

Symptoms: The password is prompted for twice for authentication that is falling over to the line password.

Conditions: This symptom is observed when login authentication has the line password as fallback and RADIUS as primary. For example:

aaa authentication login default group radius line

Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example:

enable password <keyword>

aaa authentication login default group radius enable

- CSCth31271

Symptoms: A Cisco ASR router crashes with next-hop recursive.

Conditions: This symptom is observed after the following tasks are executed:

1. Configure a route-map with recursive next-hop clause for IP address (for example, 1.2.3.4).
2. Change the recursive next-hop to IP address (for example, 5.6.7.8).
3. Apply PBR with this route-map to an interface.
4. Delete the route-map.
5. Shut the interface.

Workaround: There is no workaround.

- CSCth31395

Symptoms: Frame-relay PVC stays in INACTIVE state.

Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

Workaround: There is no workaround.

- CSCth33949

Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the **clear ppp all** command.

Conditions: This symptom is observed when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the **clear ppp all** command.

Workaround: Use the **cle vpdn tunnel l2tp all** command instead.

- CSCth36740

Symptoms: A router may experience CRC and Runt errors.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2 and when the on-board GigabitEthernet interface is hard-coded to 10mb/full duplex. It is seen with the following routers: Cisco 1900 series, Cisco 2900 series, and Cisco 3900 series.

Workaround: There is no workaround.

- CSCth38699

Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce

packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-Group mappings.

- CSCth42798

Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

Workaround: There is no workaround.

- CSCth45413

Symptoms: The environmental alarm has additional hard disk drive information in the Syslog message.

Conditions: The symptom is observed when there is one of the following service modules in the system:

SM-SRE-900-K9 SM-SRE-700-K9 NME-APPRE-522-K9 NME-APPRE-502-K9 NME-APPRE-302-K9
NME-WAE-502-K9 NME-NAM-120S NME-NAM-80S NME-NAC-K9 NME-CUE NME-UMG-EC NME-UMG

Workaround: There is no workaround.

- CSCth58283

Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

Conditions: NAT is enabled.

Workaround: There is no workaround.

- CSCth62854

Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

Workaround: There is no workaround.

- CSCth65072

Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth67608

Symptoms: Some groups are missing in the MLD Proxy cache on the Proxy router.

Conditions: This symptom is observed when ipv6 mld host-proxy is applied with existing multicast routes.

Workaround: Clear the multicast routes using clear ipv6 pim topology after applying ipv6 mld host-proxy.

- CSCth69361

Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.

Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.

Workaround: There is no workaround.

- CSCth69364

Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw>

- CSCth77531

Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU utilization in the BGP-related processes for several hours (more than 2.5).

Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process uses the most CPU; also, the number of routemap-cache entries should be very high.

Router# **show ip bgp sum**

```
BGP router identifier 1.1.1.1, local AS number 4739
BGP table version is 1228001, main routing table version 1228001 604000 network
entries using 106304000 bytes of memory
604000 path entries using 31408000 bytes of memory
762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results, and the issue will not be observed.

- CSCth80893

Symptoms: POE and Air Connect (AC) on a Cisco 892FW router do not work simultaneously. You cannot connect to the AC console when POE is powered on.

Conditions: This symptom is observed on a Cisco 892FW router that has both POE and Air Connect with POE powered on.

Workaround: There is no workaround.

- CSCth82164

Symptoms: When OCSP is being used as the revocation check method for IKE, only the first connection attempt (after reboot or cache clearing of public RSA keys) undergoes an OCSP check. Subsequent revocation checks are bypassed because the peer’s public key appears to be cached indefinitely.

No CRL or other lifetime parameters are involved, OCSF should be consulted for each IKE tunnel setup.

The following messages indicate bypassing the revocation check.

```
*Jul 13 18:43:18.095: ISAKMP:(1002): peer's pubkey is cached *Jul 13
18:43:18.095: CRYPTO_PKI: Found public key in hash table. Bypassing certificate
validation
```

Conditions: OCSF configured as revocation check method for IKE.

Workaround: There is no workaround.

- CSCth86402

Symptoms: When flapping a WAN interface, the PIM tunnel disappears.

Conditions: This happens when flapping a WAN interface after a few hours of working.

Workaround: Disable multicast routing, then enable it again.

- CSCth87587

Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

Workaround: There is no workaround.

Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth87638

Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

Conditions: The symptom is observed on WIC-based platforms. It was seen originally on an IAD243x using a HWIC-CABLE-D-2.

Workaround: Manually change the MAC address problem card.

Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- CSCth91984

Symptoms: Standby resets continuously.

Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

Workaround: Unconfigure the **set extcommunity** command.

- CSCth99237

Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

Conditions: The symptom is observed under the following conditions:

1. If the client starts to send LCP echo requests during the PPP Authentication phase.
2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

Workaround: There is no workaround.

- CSCti08336

Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are “IN” policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go “Out” of policy.

Workaround: There is no workaround.

- CSCti10016

Symptoms: After the **format** command is run on a 32-GB or larger disk, the **show** command displays that only 4 GB is free on the device.

Conditions: The symptom is observed when formatting disk that is larger than 32 GB in capacity.

Workaround: Use a smaller size disk that has no more capacity than 32 GB.

- CSCti10222

Symptoms: The following exceptions are seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of XXXX bytes failed from 0xYYYYYYYY, alignment
# Pool: I/O Free: # Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause:
No Alternate pool -Process= "IGMP Snooping Receiving Process", ipl= #, pid= #,
-Traceback= 0x81E8B6BCz 0x81EB0660z 0x802EC198z 0x802EC8E4z 0x802ED88Cz 0x802F1988z
0x803BBD88z 0x803BBF2Cz 0x8045E5CCz 0x804615F4z
```

```
Can't duplicate packet
Can't duplicate packet
Can't duplicate packet
```

Conditions: This symptom is observed when VLANs are added while multicast traffic is flowing through the router.

Workaround:

1. Prune the multicast feed that is coming from the respective VLAN using the following command:

switchport trunk allowed vlans except mcast-vlan#

or

2. Upgrade to Cisco IOS Release 15.1(2)T1.

- CSCti13286

Symptoms: Putting this configuration on a router:

```
router rip
version 2
no validate-update-source
network 10.0.0.0
no auto-summary
!
address-family ipv4 vrf test
no validate-update-source
network 172.16.0.0
no auto-summary
version 2
exit-address-family
```

and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti19627

Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

Workaround: Remove “call-park system application”.

- CSCti22190

Symptoms: The EIGRP autonomous system command does not NVGEN.

Conditions:

```
interface Tunnel2
 ip vrf forwarding vpn2
 no ip next-hop-self eigrp 10
```

Now configure the address-family ipv4 command under legacy mode. For example:

```
router eigrp 10
 no auto-summary
 address-family ipv4 vrf vpn2
 no auto-summary
```

Now show the running configuration; the autonomous system command is not NVGENed.

Workaround: Use the “address-family ipv4 vrf vpn2 autonomous 10” command.

- CSCti25280

Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

```
**ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
```

Conditions: The symptom is observed when there is also a VWIC installed in the chassis (example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

Workaround: Remove the VWIC.

- CSCti26202

Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

Conditions: The symptom is observed on a Cisco 3900 series router.

Workaround: There is no workaround.

- CSCti27128

Symptoms: A Cisco 2911 router crashes repeatedly when trying to boot up.

Conditions: This symptom occurs when an IPVS module is installed in the NME slot with an SM-NM adaptor in a Cisco 2911 router. The Cisco 2921 is not affected.

Workaround: There is no workaround if the IPVS module is required. Otherwise, the IPVS module can be removed from the Cisco 2911.

- CSCti34627

Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.

Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.

Workaround: Disable GR.

- CSCti45042

Symptoms: When the “reload warm file flash0:<image>” command is issued on a Cisco 3900e router, the router does not boot the specified image due to “System received a Bus Error exception.”

Conditions: This symptom is observed in a Cisco IOS Release 15.1(2.13)T image when the “reload warm file flash0:<image>” command is issued.

Workaround: There is no workaround.

- CSCti47649

Symptoms: A router may crash with the message:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04

Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

Workaround: There is no workaround.

- CSCti54173

Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

Conditions: The symptom is observed on a Cisco 7200 series router.

Workaround: There is no workaround.

- CSCti55261

Symptoms: On a phone button that has an overlay with call waiting DN's configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

Conditions: The symptom is observed on a phone button that has an overlay with call waiting DN's and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

Workaround: There is no workaround.

- CSCti69008

Symptoms: When dampening is configured for many VRFs, doing full vpv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

Conditions: Dampening configuration changes for VRFs.

Workaround: There is no workaround.

- CSCti72836

Symptoms: The router crashes when removing an ACL.

Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hash table.

Workaround: There is no workaround.

- CSCti86169

Symptoms: A device that is acting as a DHCP relay or server crashes.

Conditions: This symptom is observed when the “no service dhcp” command is configured.

Workaround: There is no workaround.

- CSCti89571

Symptoms: The WAAS feature cannot be enabled the first time for a new evaluation license.

Conditions: This symptom occurs when the evaluation license has not been activated.

Workaround: Enter the waas enable command twice on the interface of the NGWO device.

- CSCti90602

Symptoms: The PPTP connection is not getting established when “ip nat outside” is configured on the NAT router. The NAT router is between the client and the server.

Conditions: This symptom is observed only with the PPTP connection; all other traffic works fine.

Workaround: There is no workaround.

- CSCti93398

Symptoms: A Cisco 1861 router reloads.

Conditions: The reload occurs upon booting.

Workaround: There is no workaround.

- CSCti96028

Symptoms: A build failure is seen due to the fix committed using CSCti67511 (“Borghetti DSL PHY Firmware upgrade through usb flash”).

Conditions: When you try to build Cisco 180x platform IOS images.

Workaround: There is no workaround.

- CSCtj07125

Symptoms: Cisco IOS WAAS Express uses the burned-in MAC address of the first Ethernet interface as its own local device ID. This device ID is sent as a router identifier to the WAAS Central Manager (WCM) and is communicated to other WAAS peers during autodiscovery.

On Cisco 1941W platforms, the burned-in MAC address of the first Ethernet interface is 0000.0000.0007, which happens to be the same for all Cisco 1941W routers.

This will cause the WCM to have two routers that are registered with the same client ID. It might also affect IOS-WAAS operation.

Conditions: This symptom is observed while registering WAAS on Cisco 1941W platforms with the WCM and enabling WAAS on these platforms.

Workaround: There is no workaround.

- CSCtj07885

Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

Workaround:

- 1) Configure CME-as-SRST with “srst mode auto-provision all”.
- 2) Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:
 - a) Stop the MIB on the NMS device that is doing the polling.
 - b) Turn off SNMP polling on the device.
 - c) Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj25649

Symptoms: Inline power to ip phone fails on NM-16-ESW and NMD-36-ESW

Conditions: This symptom is seen on NM-16-ESW and NMD-36-ESW that is using a 15.1(2)T1.1 image.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T1

Cisco IOS Release 15.1(2)T1 is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T1 but may be open in previous Cisco IOS releases.

- CSCtd59027

Symptoms: The device crashes due to a bus error.

Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCte86038

Symptoms: High CPU utilization for ATM OAM timer process.

Conditions: The symptom is observed with a scaled L2 VC configuration.

Workaround: Increase the AIS RDI timeout with higher number of up and down retries.

- CSCte94301

None

Symptoms: IPv6 PBR is not applied to locally-originated ping packets.

Conditions: This symptom occurs when IPv6 PBR is configured for application to locally-originated ping packets.

Workaround: There is no workaround.

- CSCtg63096

Symptoms: The **deny ip any any fragments** command shows a high number of hits for traffic that may not be truly fragmented.

Conditions: This symptom occurs when “deny ip any any fragments” may be configured at the top of the ACL.

Workaround: There is no workaround.

- CSCtg71332

Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

Workaround:

1. Use SP services feature set.
2. Upgrade router to Cisco IOS Release 12.4(24)T.
3. Install one or more PVDM sLOTS.

- CSCtg83932

Symptoms: “Encapsulation aal5auto” may not be enabled under svc mode.

Conditions: This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 15.1(2)T.

Workaround: There is no workaround.

- CSCth15268

Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.

Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit on.

Workaround: Set “llc2 local-window” to 1.

- CSCth33500

Symptoms: NAS port is reported as zero on LNS.

Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

Workaround: There is no workaround.

- CSCth33804

Symptoms: Traffic is dropped at CPP with error message “noipv4route” after RP switchover, and traffic on few sessions is dropped.

Conditions: This symptom occurs when VRF is configured for PPPoE sessions and RP switchover is done with traffic flowing.

Workaround: Do not configure VRF.

- CSCth35377

Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

Conditions: This symptom is observed on a GigabitEthernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters: encapsulation dot1Q xxx ip pim sparse-mode.

Workaround: Remove “ip pim sparse-mode.”

- CSCth42594

Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

Conditions: The symptom is observed with the following conditions:

1. When multilink is bundled with more than one serial interfaces (not seeing this issue with only one serial interface).
2. Seeing this issue from 1500 and above (not seeing this issue when configure and remove “ppp multilink mrru local 1499”).

Workaround: There is no workaround.

- CSCth64589

Symptoms: The memory allocated at `bds_create_link_list` & `udb_create_ds` was leaked. The service policy would not be attached on the interface.

Conditions: This symptom is seen in Cisco routers loaded with Cisco IOS version of Release 15.1(2.5)T. This happens in corner case configurations where the parent class map has only one filter, which is a nested class.

Workaround: The following configuration can be modified to make things work.

```
class-map c1
class-map c2
  match class c1
```

```
policy-map p1
  class c2
```

Replace the above configuration as follows:

```
class-map c1

policy-map p1
  class c1
```

The results are the same.

- CSCth67811

Symptoms: Acct-Terminate-Cause is set as “nas-error” in Tunnel stop record when admin clear.

Conditions: This symptom is seen with admin clear tunnel using the **clear vpdn tunnel l2tp all** command.

Workaround: There is no workaround.

- CSCth78630

Symptoms: Call manager or other SAF clients are not able to learn SAF patterns.

On the forwarder, “show eigrp service-family external-client” displays multiple expired client registrations. The keepalive timer on the stale registrations is 0, and the “Client API Handle” is “0”, however the File Descriptor is still listed in the table. See the following example:

```
abi-4506#sh eigrp service-family external-client
SAF External Clients
Client Label                Client API Handle      File Descriptor
ABI_SAF_CLIENT1             0                      1
```

```

ABI_SAF_CLIENT1          0          2
ABI_SAF_CLIENT1          0          3
ABI_SAF_CLIENT1          0          4
ABI_SAF_CLIENT1          0          5
ABI_SAF_CLIENT1          0          6
ABI_SAF_CLIENT1          0          7
ABI_SAF_CLIENT1          0          8
ABI_SAF_CLIENT1          0          9
ABI_SAF_CLIENT1          0         10
ABI_SAF_CLIENT1          0         11
ABI_SAF_CLIENT1          0         12
ABI_SAF_CLIENT1          0         13
ABI_SAF_CLIENT1          0         14
ABI_SAF_CLIENT1          15         15
ABI_SAF_CLIENT1          16         16
abi-4506#

```

Using the **debug voice saf** command or the **<debug eigrp service-family [external-client {client|messages|protocol}]** command shows the following traceback:

```

%SCHED-3-STUCKMTMR: Sleep with expired managed timer 229C03BC, time 0xF2968
(4d20h ago).
-Process= "SAF-EC FORWARDER", ipl= 4, pid= 235
-Traceback= 11A14818 11A14E3C 11130E54 109A0594 10997584

```

Conditions: This symptom occurs when a SAF client unregisters/re-registers to a SAF forwarder.

Workaround: Reload the router acting as forwarder and ensure there is no unregister/re-register activity on the client (for example, do not restart publishing/subscribing services, etc.).

- CSCth83508

Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

Conditions: The problem is seen when using WSMA to run the **session install** command.

Workaround: Perform the install manually from a vty session.

- CSCti17190

Symptoms: A router crashes when we try to do sre install.

Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

Workaround: There is no workaround.

- CSCti18193

Cisco IOS-Æ Software Release, 15.1(2)T is affected by a denial of service (DoS) vulnerability during the TCP establishment phase. The vulnerability could cause embryonic TCP connections to remain in a SYNRCVD or SYNSENT state. Enough embryonic TCP connections in these states could consume system resources and prevent an affected device from accepting or initiating new TCP connections, including any TCP-based remote management access to the device.

No authentication is required to exploit this vulnerability. An attacker does not need to complete a three-way handshake to trigger this vulnerability; therefore, this vulnerability can be exploited using spoofed packets. This vulnerability may be triggered by normal network traffic.

Cisco has released Cisco IOS Software Release 15.1(2)T0a to address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100812-tcp>

- CSCti18745

Symptoms: If user has configured http port 80 or default http port, then reboots the router, it will produce invalid connection url with port 0. Later the connection from ACS to CPE might fail.

Conditions: This symptom occurs if user has default http port 80 configured and then reboots the router.

Workaround: Once router is up and running, again configure some port other than 80, and then reconfigure port 80.

```
Router(config)#ip http port 8000
```

```
Router(config)#no ip http port or ip http port 80
```

- CSCti25063

Symptoms: Call drops after codec change through midcall INVITE.

Conditions: This issue occurs when both the codec and direction are changed compared to previous negotiated SDP. This is seen when using Cisco Unified Border Element (CUBE) with Cisco IOS Release 15.1(2)T. See the following topology:

SIP(1) -- CUBE -- SIP(2)

Codec G711 is negotiated.

Next on SIP(2) midcall INVITE is received with updated SDP.

CUBE detects updated SDP but when sending out INVITE on SIP(1), the SDP still has previous codec G711.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T0a

Cisco IOS Release 15.1(2)T0a is a rebuild release for Cisco IOS Release 15.1(2)T. The caveats in this section are resolved in Cisco IOS Release 15.1(2)T0a but may be open in previous Cisco IOS releases.

- CSCti18193

Cisco IOS Software Release 15.1(2)T is affected by a denial of service (DoS) vulnerability during the TCP establishment phase. The vulnerability could cause embryonic TCP connections to remain in a SYNRCVD or SYNSENT state. Enough embryonic TCP connections in these states could consume system resources and prevent an affected device from accepting or initiating new TCP connections, including any TCP-based remote management access to the device.

No authentication is required to exploit this vulnerability. An attacker does not need to complete a three-way handshake to trigger this vulnerability; therefore, this vulnerability can be exploited using spoofed packets. This vulnerability may be triggered by normal network traffic.

Cisco has released Cisco IOS Software Release 15.1(2)T0a to address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100812-tcp>

Open Caveats—Cisco IOS Release 15.1(2)T

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(2)T. All the caveats listed in this section are open in Cisco IOS Release 15.1(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtb55576

Symptoms: When a HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

Workaround: There is no workaround.

- CSCtb70595

Symptoms: A Cisco router may experience a crash.

Conditions: This symptom has been observed on a Cisco 2851 running Cisco IOS Release 12.4(25a).

Workaround: There is no workaround.

- CSCtb79492

Symptoms: A Cisco AS5400XM is seeing high CPU due to process background load.

Conditions: This symptom is observed when calls are flowing through this router and the router is trying to access Flash to pull the sound files.

Workaround: End all voice calls coming to the box, or reload the box.

Further Problem Description: Steps to Recreate:

1. Use the **more flash:XXX** command
2. Observe the CPU utilization increase back to 100%.

- CSCtc06935

Symptoms: Packet loss occurs between two Cisco Catalyst 3200 MAR routers connected over FESMIC Fast Ethernet ports via wireless radios after upgrading to Cisco IOS Release 12.4(22)T2.

Conditions: The symptom is observed with the following conditions:

- After a code upgrade.
- On Cisco Catalyst 3200s connected via wireless radios.
- It does not occur on devices directly connected via fiber.

Workaround: Use Cisco IOS Release 12.4(1a).

- CSCtc52299

Symptoms: UDP packets broadcast with destination port 53 for 10 minutes. It brings the CPU to 100% and causes router to crash if DNS server is removed.

Conditions: This symptom is observed With UDP broadcast at port 53 cause the port remain open and CPU hog in 5-10 minutes Router CPU reaches to 100% and does not come down even you stop the broadcast traffic

Workaround: There is no workaround.

- CSCtd59027

Symptoms: The device crashes due to a bus error.

Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCtd62885

Symptoms: IKE renegotiation might fail for minutes while having one peer display:

```
%CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from <ip> was not encrypted and it should have been
```

Conditions: This symptom is observed when certificates are used. The signature verification might fail after MM5 or MM6 messages are exchanged preventing the tunnel establishment. The issue seems to affect Cisco IOS Release 12.4(20)T3 and Release 12.4(24)T2 images as well.

Workaround: Use pre-shared keys.

- CSCtd90030

Symptoms: A Cisco 2851 router may crash with a bus error.

Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCte17560

Symptoms: Offered rate in QoS class shows unusually high values.

Conditions: The symptom is observed when service-policy is applied on a multilink interface.

Workaround: There is no workaround.

- CSCte50870

Symptoms: A Cisco AS5400 crashes due to watchdog timeout. CPU hogs due to the “SERIAL A detect” process are seen before the reload:

```
%SYS-3-CPUHOG: Task is running for (36000)msecs, more than (2000)msecs (36/6), process = SERIAL A'detect.
```

After some time the device crashes:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SERIAL A'detect.
```

Conditions: This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.4(24)T2. The serial interfaces of the device are configured with the **autodetect encapsulation xxx** command.

Workaround: If possible, remove this command to avoid the crashes.

- CSCte89130
Symptoms: Router experiences a memory leak.
Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).
Workaround: There is no workaround.
- CSCte93792
Symptoms: Virtual access bound to an ATM interface does not come up.
Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.
Workaround: There is no workaround.
- CSCte94221
Symptoms: PPP connection over CDMA link is flapping.
Conditions: This symptom is observed with Cisco IOS Release 15.0M.
Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface and wait for 2 minutes.
- CSCtf28796
Symptoms: With async_dialer interface type, PPP fails.
Conditions: This issue is seen only with async_dialer interface type. There is no issue with async_legacy and async_virtual interface types.
Workaround: There is no workaround.
- CSCtf41721
Symptoms: A DMVPNv6 hub might crash when doing a **shutdown** followed by a **no shutdown** on the tunnel interface of the other hub. DMVPNv6 hub crashes at ifs_lookup_prefix_common.
Conditions: This symptom is observed when DMVPNv6 is configured with 2 hubs and 2 spokes. Hub 2 tunnel is shut and unshut, and hub 1 crashes.
Workaround: There is no workaround.
- CSCtf50867
Symptoms: A Cisco router reloads at iprouting_is_hdvrf_idb.
Conditions: This symptom is observed when configuring pri-group nfas_d with Cisco IOS Release 15.1(01.05)T.
Workaround: There is no workaround.
- CSCtf94403
Symptoms: Input buffer drops and throttles are observed on an onboard FastEthernet interface and HWIC ethernet interface of a Cisco 2801 under low traffic conditions.
Conditions: This symptom appears to be related to the router fragmenting packets, which causes the interface particle pool and then the Normal fallback pool to fill up.
Workaround: There is no workaround.
- CSCtg06045
Symptoms: A Cisco IOS router may reload when changing crypto ACL configuration. Crash traceback is seen from the crypto ACL process.

Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T12 with a high CPU stress load.

Workaround: The workaround is to simplify and consolidate the ACE entries in the crypto ACL. Also, reducing the CPU stress level may help.

Further Problem Description: This is very specific to the ACE entries in crypto ACL downloaded from KS. Its pattern of deny alternating host to any and any to host could be part of the root cause.

- CSCtg41606

Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multiaccess interface (for example, Ethernet), then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

Conditions: This symptom is observed when the upstream device does not support proxy arping.

Workaround: Use the **reverse-route remote-peer next-hop-ip** command instead of the **reverse-route** command.

- CSCtg42271

Symptoms: A router running Cisco IOS Release 15.0(1)M1 may experience a series of spurious memory access errors and a bus error when configured for IPS:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0xFFFFFFFF reading 0XXX
%ALIGN-3-TRACE: -Traceback= 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF 0xFFFFFFFF
0xFFFFFFFF

%ALIGN-1-FATAL: Illegal access to a low address 13:35:23 CDT Tue Apr 20 2010
addr=0x70, pc=0x251A00CCz , ra=0xFFFFF3331z , sp=0x28F88EB0

%ALIGN-1-FATAL: Illegal access to a low address 13:35:23 CDT Tue Apr 20 2010
addr=0x70, pc=0x251A00CCz , ra=0xFFFFF3331z , sp=0x28F88EB0

XX:XX:XX XXX XXX XX XXXX: TLB (store) exception, CPU signal 10, PC = 0xFFFFFFFF
<snip>
```

Conditions: This symptom is observed on devices configured for IPS and running Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

- CSCtg42904

Symptoms: After applying the flow monitor to a virtual-template interface, a Cisco router crashes with the following error message:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

Conditions: This symptom is observed on a router configured with EasyVPN.

Workaround: There is no workaround.

- CSCtg49868

Symptoms: CUBE does not pass the RTP in both directions between two pbx devices

Conditions: This symptom is observed with the following topology:

```
PbxA (SAP BCM)---SIP--->CUBE---SIP--->PbxB(OCS 2007 R2)
```

This problem is specific to the two third-party vendor SIP servers, SAP BCM and OCS 2007 R2. This problem only occurs when making a call from pbxA (SAP BCM) to pbxB(OCS 2007 R2). The call is okay from pbxB(OCS 2007 R2) to pbxA (SAP BCM).

Workaround: Use E1 loop.

- CSCtg54606

Symptoms: Ping fails over a serial interface with x25 encapsulation.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(1.10)T.

Workaround: There is no workaround.

- CSCtg55338

Symptoms: If a router is reloaded with a GRE tunnel interface configured with tunnel protection and a dialer interface as the tunnel source, the crypto socket is not created and IPSec is not triggered.

Conditions: This symptom is observed after reload. A router crypt socket is missing.

Workaround: After the reload, remove and reapply the tunnel protection on each tunnel interface.

- CSCtg59158

Symptoms: Router console is flooded with the following error messages:

```
crypto_engine_ps_vec: DF_BIT_STATUS_OK Check failed
crypto_engine_ps_vec: DF_BIT_STATUS_OK Check failed
```

Conditions: This symptom is observed when new SAs are installed during rekeys or after clearing existing SAs. This symptom is observed when GETVPN (crypto map) is configured along with WAAS.

Workaround: Cryptomaps are currently not supported in the current phase of WAAS-Express. Use VTI or unconfigure WAAS-Express.

- CSCtg65423

Symptoms: SS7 and RUDP backhaul fails to bring up links correctly on Cisco IOS Release 15.1T.

Conditions: This symptom is observed in Cisco IOS Release 15.1T with interworking with PGW.

Workaround: Install Cisco IOS Release 12.4T.

- CSCtg66989

Symptoms: NDR performance is degraded by 10% on GRE with IPSec.

Conditions: This symptom is observed on GRE with IPSec.

Workaround: There is no workaround.

- CSCtg67146

Symptoms: File transfer to the flash fails with a “TF I/O failed in data-in phase” message. The **archive** command fails 100% of the time, whereas a **copy** command is successful sometimes.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(24)T or above and with an STI flash 7.2.0. The transfer fails with some delay (~50-100msec).

Workaround:

- Transfer without a delay is successful.
- Transfer with Cisco IOS Release 12.4(9)T is successful.
- Transfer with a newer flash card (tested with Sandisk 8.0.0) is successful.

Further Problem Description: This symptom is also observed with Cisco IOS Release 12.4(24)T, Release 12.4(24)T1, Release 12.4(24)T2, Release 12.4(24)T3 and Release 15.1(1)T.

- CSCtg68568

Symptoms: A Cisco 3945 router configured as a GETVPN group member might crash when passing stateful traffic.

Conditions: This symptom occurs when fragmentation of the IP datagram is required due to an MTU limit of 1500 bytes.

Workaround: Configure hosts to negotiate lower TCP MSS (1360) bytes and avoid fragmentation.

- CSCtg71332

Symptoms: Using NM-1T3/E3-T3 controller will be down/down on Cisco 3800 ISR routers.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

Workaround:

1. Use SP services feature set.
2. Upgrade to Cisco IOS Release 12.4(24)T.
3. Install one or more PVDM slots.

- CSCtg72455

Symptoms: Async interface for an internal V.92 modem on a Cisco 1811 router freezes for approximately 5 to 30 minutes, but eventually fixes itself.

Conditions: This symptom is observed on a Cisco 1811 router that is running Cisco IOS Release 15.0 and above.

Workaround: Disable the V.44 compression by configuring the Cisco 1800/890 modem to negotiate V.42bis by using the following modemcap:

```
1811 V.92 modemcap:
modemcap entry V.42bis:MSC=&F\N4%C0+DS=3
Sample chat-script:
chat-script dial "" "ATD\T" TIMEOUT 60 CONNECT \p
```

The following is a sample line configuration to apply the above chat-script:

```
line 1
 script dialer dial
 modem InOut
 no exec
 transport input all
 transport output all
 stopbits 1
 speed 115200
 flowcontrol hardware
```

- CSCtg75710

Symptoms: BGP convergence time is about 8% greater than in unaffected releases.

Conditions: This symptom is observed only when BGP is configured. It is most notable when using VPNv4 with hundreds of VRFs and hundreds of thousands of networks.

Workaround: Wait a little bit longer for BGP to converge.

- CSCtg78691

Symptoms: A Cisco SPA525G IP phone communicating via SSL VPN from a remote office is experiencing choppy and poor quality audio.

Conditions: This symptom is observed on a Cisco SPA525G IP phone running firmware version 7.4.3 on Cisco Unified CME 8.0. The symptom is observed only when the phone is connected via SSL VPN; the audio quality of the same phone connected in the LAN network is clear.

Workaround: There is no workaround.

Further Problem Description: Choppy audio is heard by the Cisco SPA525G as well as the PSTN party when the Cisco SPA525G connects to the corporate network via SSL VPN. The first 10 seconds of the audio is clear, and then the choppiness starts. The CPU spikes to over 90% due to SSLVPN_PROCESS.

- CSCtg81560

Symptoms: A Cisco router crashes.

Conditions: This symptom is observed when Cisco IOS firewall is configured.

Workaround: There is no workaround.

- CSCtg83804

Symptoms: A Cisco router crashes when uploading files larger than 1 MB via WebVPN.

Conditions: This symptom is observed when CEF and the crypto engine are enabled.

Workaround: Disable the CEF and/or disable the crypto engine.

- CSCtg84222

Symptoms: The VRF tunnel flaps when attaching the QOS policy in the tunnel. This problem can cause traffic drop on a tunnel over an ATM subinterface when a service policy is installed.

Conditions: This symptom occurs when a service policy is attached to an ATM sub interface and the router has OSPF or EIRGP routing protocol configured. Both the subinterface and routing protocol need to be in the same VRF.

Workaround: There is no workaround.

- CSCtg89893

Symptoms: A Cisco router may reload due to a bus error:

Conditions: This symptom is observed on a Cisco 2811 router that is running Cisco IOS Release 12.4(22)T3.

Workaround: There is no workaround.

- CSCtg90518

Symptoms: The output of “sh ip inspect statistics” shows negative or irrelevant value(s). The following log is generated:

```
%FW-4-ALERT_ON: getting aggressive, count (6/2147483647) current 1-min rate:
4294967295
```

Conditions: This symptom is observed on Cisco IOS Firewall on Cisco IOS Release 15.0(1)M where ip inspect tcp is enabled.

Workaround: There is no workaround.

- CSCtg92548

Symptoms: The D-channel in the PRI module loses “receive” from the carrier and the controller goes down. If HWE CAN DSP is down or crashed, then the D-Channel “receive” data stream would not be passed from the multiflex trunk (MFT) RX input to the IOS PRI Controller, which matches the symptom that was observed.

Conditions: This symptom is observed on an MFT equipped with HWE CAN. The failure occurs intermittently; this failure occurred 6 months after the last HWE CAN failure.

Workaround: Remove HWE CAN from the MFT module.

- CSCth03379

Symptoms: A Cisco router reloads while booting with DSL configurations.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.1(1.15)T and configured with a DSL controller.

Workaround: There is no workaround.

- CSCth04187

Symptoms: FTP (both active and passive) to the Internet fails.

Conditions: This symptom is observed on a Cisco router with inspect and crypto map configured on public interface, and an access-group on the inside interface. When the crypto map is applied on the public interface, FTP fails. As soon as we remove the crypto map, FTP works.

Workaround: Remove the crypto map from the public interface.

- CSCth06209

Symptoms: A Cisco router reloads in a loop.

Conditions: This symptom is observed when WAAS is enabled in the configuration and traffic is flowing through the box, and the router is then reloaded using a laptop.

Workaround: Disconnect the laptop from the router and hard reset the router.

- CSCth07336

Symptoms: Data calls cannot be dialed when using E1 PRI on a Cisco 2911 router with VWIC2-1MFT-T1/E1. The call lasts for 22 seconds and when using PPP, LCP fails to negotiate.

Conditions: This symptom is observed when using E1 PRI for making data calls; HDLC as well as PPP have the same issue, but data calls can be made with the T1 PRI.

Workaround: There is no workaround.

- CSCth09876

Symptoms: Cisco IOS IP Service Level Agreements (SLAs) cannot be auto-discovered if IP SLAs are removed from the responder first.

Conditions: This symptom is observed on a Cisco device after IP SLAs have been unconfigured. Subsequent attempts to reconfigure the device as an IP SLAs responder fail.

Workaround: Reload the router and configure the device as an IP SLAs responder.

- CSCth10764

Symptoms: PPP negotiation is not working correctly between a Cisco 7200 router and a Cisco GSR XR blade.

Conditions: This symptom is observed when the max-header size is different on both ends; PPP does not negotiate the lower size.

Workaround: There is no workaround.

- CSCth12935

Symptoms: Input CoPP alone does not work for MPLS-VPN tagged packets. All packets match the default “class-default” class. However, if output CoPP is configured together with input CoPP, input CoPP works fine for MPLS-VPN tagged packets. Packets match the intended user-configured class and can be dropped.

Conditions: This symptom is observed in Cisco IOS Release 12.4 since Release 12.4(23) on the Cisco 7200 series router. In Cisco IOS Release 12.4 releases older than Release 12.4(23), input CoPP does not work at all for MPLS-VPN tagged packets, even if output CoPP is also configured together with input CoPP.

Workaround: There is no workaround.

- CSCth13153
Symptoms: An incorrect UDLR reporter occurs on a Cisco router that is connected to a UDLR link and PIM-SM domain with auto-RP configurable.
Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 15.1(1)T1.
Workaround: There is no workaround.
- CSCth15519
Symptoms: A Cisco router reloads with **show memory address_value** command.
Conditions: This symptom is observed on a Cisco 1861 router.
Workaround: There is no workaround.
- CSCth16539
Symptoms: A Cisco device crashes.
Conditions: This symptom is observed a few hours after multiple T1s are configured in a multilink PPP bundle.
Workaround: Do not use HDLC encapsulation or remove outbound service-policy from any HDLC-encapsulated serial interfaces.
Further Problem Description: The Cisco device has traffic coming in a multilink PPP bundle with multiple T1s. This traffic exits out of an HDLC serial interface with an outbound service-policy applied to that interface, eventually causing a crash.
- CSCth16962
Symptoms: The primary KS KEK timer will get stuck after a GDOI policy change, resulting in repeated rekeys. This symptom seems to occur even after a failure in the key servers
Conditions: This symptom is observed with repeated rekeys to GMs.
Workaround: There is no workaround.
- CSCth18189
Symptoms: A Cisco router crashes when multiple SVIs are created and deleted using the **interface range** command.
Conditions: This symptom is observed when a Cisco EHWIC-D-8ESG card is present in the router and a user tries to create and delete multiple SVIs using the **interface range** command.
Workaround: There is no workaround.
- CSCth19516
Symptoms: A Cisco router crashes when PFR is configured and there is a changeover from primary to fallback link.
Conditions: This symptom is observed when PFR is configured with link group.
Workaround: Remove the PFR link group and use traditional routing instead of PFR.
- CSCth20018
Symptoms: A Cisco router crashes after configuring and removing the onboard GE subinterface.
Conditions: This symptom is observed on a Cisco router with a basic configuration.
Workaround: There is no workaround.

- CSCth20696

Symptoms: An address Error (load or instruction fetch) exception occurs (CPU signal 10).

Conditions: This symptom is observed on a Cisco 7204vrx router with an NPE-G1 that is running Cisco IOS Release 12.4(25c).

Workaround: There is no workaround.

- CSCth23354

Symptoms: Packets are not reaching the proper queue.

Conditions: This symptom is observed when class-map is configured with VLAN.

Workaround: There is no workaround.

- CSCth23908

Symptoms: QSIG APDU in PRI release message in SIP 603 is not passed to PRI side.

Conditions: This symptom is observed in SIP 603 in the release message on egress PRI side.

Workaround: There is no workaround.

- CSCth26441

Symptoms: Non-broadcast Ethernet frames are dropped by the Gig1/0 controller that connects to the NME module.

Conditions: This symptom is observed when xconnect is configured on a subinterface and 802.1q trunking is used to connect to the NME module.

Workaround: There is no workaround.

- CSCth27442

Symptoms: A Cisco router crashes when flapping ACL with traffic flowing.

Conditions: This symptom is observed on a Cisco 7200 series router running Cisco IOS Release 15.0(1)M2 with the following configuration:

```
no access-list 12 permit 192.1.1.170
no access-list 112 permit ip host 192.1.1.249 any
ip access-list extended dc-gab
no deny ip any 192.15.2.0 0.0.0.255
no permit ip any 192.235.0.0 0.0.255.255
ip access-list extended dc-sli
no deny ip any 192.22.1.0 0.0.255.255
no permit ip any 192.222.0.0 0.0.255.255
no ip access-list extended dc-sli
no ip access-list extended dc-gab
access-list 12 permit 192.1.1.170
access-list 112 permit ip host 192.1.1.249 any
ip access-list extended dc-gab
deny ip any 192.15.2.0 0.0.0.255
permit ip any 192.235.0.0 0.0.255.255
ip access-list extended dc-sli
deny ip any 192.22.1.0 0.0.255.255
permit ip any 192.222.0.0 0.0.255.255
```

Workaround: Remove the ACL without removing the ACEs first by entering the **no ip access-list extended dc-gab** command. If you flap the ACL configuration in the following way, it is equivalent of the original configuration, but it will NOT crash the router:

```
conf t
no access-list 12 permit 192.1.1.170
no access-list 112 permit ip host 192.1.1.249 any
```

```

no ip access-list extended dc-sli
no ip access-list extended dc-gab
access-list 12 permit 192.1.1.170
access-list 112 permit ip host 192.1.1.249 any
ip access-list extended dc-gab
deny ip any 192.15.2.0 0.0.0.255
permit ip any 192.235.0.0 0.0.255.255
ip access-list extended dc-sli
deny ip any 192.22.1.0 0.0.255.255
permit ip any 192.222.0.0 0.0.255.255

```

- CSCth28007

Symptoms: Cisco IP phone users may experience dropped calls, resetting phones, and one-way audio.

Conditions: These symptoms are observed on a Cisco 3825 router that is running Cisco IOS Release 15.1(1)T and CME 8.0 when there are 4 or more active calls. The symptoms occur with the following topology:

```
Router/ PBX ---pri---- CISC03825 ----sccp---- ip phone.
```

It is a normal external call: PSTN <----> IP phone calls.

Workaround: Install Cisco IOS Release 12.4(15)XZ2 or another release earlier than Release 15.n.

Further Problem Description: With “term mon” turned on, the following message is displayed and IP phones are deregistered from CME:

```

%C5510-4-NO_RING_DESCRIPTOR: No more ring descriptors available on slot 0 dsp 3.
%C5510-4-NO_RING_DESCRIPTOR: No more ring descriptors available on slot 0 dsp 3.
%IPPHONE-6-REG_ALARM: 10: Name=SEP00235EB6BC89 Load= SCCP70.8-5-3S Last=TCP-timeout
%IPPHONE-6-UNREGISTER_ABNORMAL: ephone-7:SEP00235EB6BC89 IP:10.0.3.130 Socket:5
DeviceType:Phone has unregistered abnormally.

```

Test calls indicate that the router behaves normally when there are 3 or fewer active calls. As soon as a fourth active call is established, however, users may lose access to the router (no icmp ping respond), or experience one-way audio or phones deregistering from CME.

When the symptoms occur, the **show process cpu** command indicates that the router CPU utilization has gone above 90%. The problem is resolved as soon one of the active calls is dropped and there are 3 or fewer active calls.

- CSCth30648

Symptoms: HWIC-1ADSL is not staying connected to the provider.

Conditions: This symptom is observed on a Cisco 1841 router.

Workaround: There is no workaround.

- CSCth31395

Symptoms: A frame-relay PVC stays in INACTIVE state.

Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M2.14.

Workaround: There is no workaround.

- CSCth31939

Symptoms: A Cisco device crashes when policy map and oam-pvc manage are configured.

Conditions: This symptom is observed when policy map and oam-pvc manage are configured.

Workaround: There is no workaround.

- CSCth33500

Symptoms: NAS port is reported as zero

- Conditions: This symptom is observed when “vpdn aaa attribute nas-port vpdn-nas” is configured.
Workaround: There is no workaround.
- CSCth36114
Symptoms: A Cisco device crashes after executing “write memory” via SDM.
Conditions: This symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.
Workaround: Install Cisco IOS Release 12.4 or earlier.
 - CSCth36740
Symptoms: A Cisco device may experience CRC and Runt errors when the on-board GigabitEthernet interface is hard coded to 10mb/Full duplex.
Conditions: This symptom is observed on a Cisco 3925 that is running Cisco IOS Release 15.0(1)M2.
Workaround: There is no workaround.
 - CSCth37092
Symptoms: A crash is observed in the PKI-HA feature when standby tries to sync up with active router.
Conditions: This symptom is observed after a PKI server is created on the active router and cloning of this PKI server on the standby box occurs.
Workaround: There is no workaround.
 - CSCth37580
Symptoms: Dampening route is present even after removing bgp dampening.
Conditions: This symptom is observed in Cisco IOS Release 15.1(1)T1.
Workaround: There is no workaround.
 - CSCth38964
Symptoms: Unknown SSH session may cause the router to crash.
Conditions: Unknown. The symptom is observed during an SSH attack.
Workaround: Disable SSH or configure an access list to block invalid addresses.
 - CSCth39161
Symptoms: Duplicate NAT mappings may impact the use of IP Telephony devices operating behind NAT.
Conditions: This symptom is observed on the Cisco IAD881.
Workaround: There is no workaround.
 - CSCth44275
Symptoms: A Cisco router may reload due to memory corruption when making multiple on-ramp fax calls.
Conditions: This symptom is observed on Cisco 2900 series platforms.
Workaround: There is no workaround.
 - CSCth45413
Symptoms: The environmental alarm contains additional hard-disk drive information in the Syslog message.

Conditions: This symptom is observed when one of the following Cisco service modules is in the system:

- SM-SRE-900-K9
- SM-SRE-700-K9
- NME-APPRE-522-K9
- NME-APPRE-502-K9
- NME-APPRE-302-K9
- NME-WAE-502-K9
- NME-NAM-120S
- NME-NAM-80S
- NME-NAC-K9
- NME-CUE
- NME-UMG-EC
- NME-UMG

Workaround: There is no workaround.

- CSCth48457

Symptoms: A Cisco device may crash at qos_classify_opttype

Conditions: This symptom is observed when changes are made to the service policy while traffic is running.

Workaround: Define the policy-map you wish to run before applying it on the interface level.

- CSCth48467

Symptoms: FAX Passthrough will not up speed from G729 to G711.

Conditions: This symptom is observed when MGCP is configured. The topology is as follows:

Modem--{Telco}--[Nortel IWTSPM IP to TDM RTP]--|--[Nortel Cs2K]--|--[IAD2435]==FXS==[FAX]

Workaround: There is no workaround.

- CSCth50582

Symptoms: Dialer interfaces are not getting IP addresses from the IPCP pool after the main ATM interface flaps.

Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 15.1(2)T.

Workaround: There is no workaround.

- CSCth51143

Symptoms: A Cisco router crashes when trying to free a chunk with a non-zero refcount.

Conditions: This symptom is observed when browsing the internet through a laptop.

Workaround: There is no workaround.

- CSCth51168

Symptoms: An H.323 to H.323 CUBE may incorrectly reuse existing TCP sockets when completing H.323 calls. This leads to call failures with cause values of:

18 - No user responding; or
 102 - Recovery on timer expiry

Conditions: This symptom is observed on a Cisco 7206VXR CUBE handling 100+ calls and running Cisco IOS Release 12.4(22)T5.

Workaround: Disable reuse of TCP sockets with the **voice service voip h323 h225 timeout tcp call-idle value 0 !** command.

- CSCth52485

Symptoms: A call from the PSTN reaches an AC agent via the AC Route Point, and the call is successfully answers. The AC agent then attempts a blind transfer using the AC to another IP Phone, but after around 8 seconds of silence the call is dropped.

On the CUBE we see the following (the below messages exclude the communication between the CUCM and the CUBE as it is irrelevant):

```
<- Invite outbound to the PGW
-> 200 OK inbound from the PGW
<- ACK outbound to the PGW
<- UPDATE outbound to the PGW
-> 200 OK inbound from the PGW
<- Invite outbound to the PGW
-> 200 OK inbound from the PGW
<- ACK outbound to the PGW
<- Invite outbound to the PGW
-> 491 Request Pending inbound from the PGW
<- ACK outbound to the PGW
```

Then the CUBE receives a BYE after 8 seconds from the CUCM and forwards this to the PGW and the call terminates.

After receiving the 491 Request Pending, the CUBE is not forwarding this to the CUCM, whereas all previous SIP messages are forwarded successfully.

The CUBE should forward this 491 to the CUCM, and then the CUCM should react by sending the Invite again for which it received the 491 Request Pending.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T.

Workaround: There is no workaround.

- CSCth52720

Symptoms: Client-initiated L2TPv2, IPCP packets are not sent when MLP is enabled.

Conditions: This symptom is seen when ppp multilink is configured with Cisco IOS Release 12.4(24)T3, Release 12.4(11)XJ and Release 15.1(1)T.

Workaround: Remove ppp multilink configuration or downgrade to Cisco IOS Release 12.3(14)T6.

- CSCth53056

Symptoms: Alignment errors are seen on Cisco IOS Release 12.4(24)T1.

Conditions: This symptom is observed on Cisco 2800 but is not platform dependent.

Workaround: There is no workaround.

- CSCth54832

Symptoms: Ping fails when the clients in different VLANs communicate with each other with a packet size greater than the configured MTU size on the SVIs.

Conditions: This symptom occurs when using any MTU size less than 1500 on the SVIs.

Workaround: Configure the same MTU size in the entire path.

- CSCth55781

Symptoms: The Cisco AS5400XM gateway is rebooting due to the following error:

```
%SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP by driver having ifIndex
529 and ifDescr
```

```
Serial7/2:23-Signaling
```

Conditions: This symptom is observed on the Cisco AS5400XM gateway.

Workaround: There is no workaround.

- CSCth56502

Symptoms: A router that is running Cisco IOS may crash when executing the **show run** or **write mem** commands.

Conditions: This symptom is observed when the device has “memory record traceback” configured.

Workaround: There is no workaround.

- CSCth57542

Symptoms: The “show voice dsp command history 1/1:0” reloads Cisco AS5400XM router if slot1 is having T1 controller.

Conditions: This symptom is observed in Cisco IOS Release 15.1(2.5)T.

Workaround: Apply **show voice dsp command history** command only for the slots having PVDm.

- CSCth59156

Symptoms: In a router that is running Cisco IOS Release 15.0(1)M, it was observed that the memory got fragmented over a period of 5 weeks. The problem was seen in only one router. We are waiting for more show command outputs to investigate why the free blocks are not getting coalesced.

Conditions: This symptom is seen on a router that is running Cisco IOS Release 15.0(1)M.

Workaround: There is no workaround.

- CSCth59784

Symptoms: Process watchdog timeout crashinfo is not written on steelers box.

Conditions: This symptom occurs when process watchdog timeout crashinfo file is not written into flash for steelers platforms.

Workaround: There is no workaround.

- CSCth60192

Symptoms: A router crashes with WAAS-EX.

Conditions: This symptom occurs when configuring WAAS-EX and starting data traffic.

Workaround: There is no workaround.

- CSCth61759

Symptoms: Video call fails with CVTA.

Conditions: This symptom is observed with end-to-end SIP flow-around call with CVTA.

Workaround: There is no workaround.

- CSCth61827

Symptoms: Invalid memory action is followed by traceback when traffic is on.

Conditions: This symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 15.1(2.5)T.

Workaround: There is no workaround.

- CSCth62136

Symptoms: ISDN L2 goes to “Layer 2 NOT Activated”.

Conditions: This symptom is observed when Service-Policy is attached to the Dialer Interface.

Workaround: Remove Service-Policy from interface.

Further Problem Description: This is not seen with Cisco IOS Release 12.4(13d) and Release 12.4(15)T12.

It has been seen with Cisco IOS Releases 12.4(22)T5, 12.4(24)T3, and 15.0(1)M3.

- CSCth62157

Symptoms: Router crashes when pumping data (HTTP, TELNET, FTP). This traffic is inspected by Cisco IOS firewall, and WAAS is configured.

Conditions: This symptom is observed while pumping in continuous data traffic for a duration of one hour. This traffic is optimized by WAAS and inspected by Cisco IOS firewall.

Workaround: Remove Cisco IOS FW Zone membership under WAAS interface.

- CSCth63196

Symptoms: The sip source interface binding commands disappear after being configured and functional.

Conditions: This symptom is observed when the T1 subinterface, which is bound, flaps.

Workaround: Reapply the CLI manually.

- CSCth64468

Symptoms: V110 call fails after the previous call was terminated with +++ ATH.

We do not see the BAD-modem issue caused by CSCtg52450 anymore, but we now see NO CARRIER. See the following example:

```
NLAMSB1-LRTR01 line 0/322 DialOUT_Modems
at
OK
atz
OK
at+isp=0
OK
at+ipt=4
OK
atdi222
CARRIER RX: 9600 TX: 9600
PROTOCOL: V110
CONNECT
NLAMSB1-LRTR02>
NLAMSB1-LRTR02>
NLAMSB1-LRTR02>+++ATH
% Bad IP address or host name
% Unknown command or computer name, or unable to find computer address
NLAMSB1-LRTR02>
OK
at
OK
at
OK
atz
OK
at+isp=0
```

```
OK
at+ipt=4
OK
atdi222
NO CARRIER
```

Conditions: This symptom is seen when V110 call fails after the previous call was terminated with +++ ATH.

Workaround: Use Cisco IOS **exit** or **logout** commands.

Further Problem Description: Log when doing the first call and after braking it with +++ ATH:

```
%CALLRECORD-3-V12_TERSE_CALL_REC: DS0
slot/contr/chan=0/0/30, slot/port=0/322, call_id=1, userid=(n/a), ip=0.0.0.0,
calling=221, called=222, std=V110, prot=None, comp=None, init-rx/tx
b-rate=9600/9600, finl-rx/tx b-rate=9600/9600, rx/tx chars=0/0, retx=0,
retx-per-frame=0, local-retrains=0, remote-retrains=0, local-rate-reneg=0,
remote-rate-reneg=0, time=0h 0m 14s, disc(modem)=0 Normal hang-up

%ISDN-6-CONNECT: Interface Serial0/0/0:30 is now
connected to 221 N/A

%ISDN-6-DISCONNECT: Interface Serial0/0/0:30
disconnected from 221 , call lasted 70 seconds
```

- CSCth65072

Symptoms: A memory leak is experienced in the big buffer pool while using the service reflection feature.

Conditions: This symptom is unknown other than service reflection is configured.

Workaround: There is no workaround.

- CSCth66251

Symptoms: Not able to configure policy-map for the second time in a Cisco 860 router.

Conditions: This symptom is observed while configuring policy-map for the second time. The Cisco 860 throws internal data base error.

Workaround: There is no workaround.

- CSCth67608

Symptoms: Some groups are missing in the MLD proxy cache on the proxy router.

Conditions: This symptom happens when the “ipv6 mld host-proxy” is applied with existing multicast routes.

Workaround: Clear the multicast routes using “clear ipv6 pim topology” after applying “ipv6 mld host-proxy”.

- CSCth67788

Symptoms: SVTI stops forwarding traffic when a local policy is configured on a device.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.0(1)M1.

Workarounds:

1. Do not use a local policy.
2. Configure “no ip route-cache cef” on the tunnel interface.

- CSCth68038

Symptoms: After a simulated failover of an L2L tunnel, a Cisco 7200 router with VSA will fail to encrypt traffic for a period of time, typically for several minutes. VSA will then begin to encrypt traffic correctly. The problem appears to be triggered when manually failing over a spoke from one hub Cisco 7200 without VSA to a secondary hub Cisco 7200 with VSA.

Conditions: This symptom is observed on a Cisco 7200 router with VSA.

Workaround: Use software encryption.

- CSCth69361

Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using Orchestrator Agent.

Conditions: This symptom is observed when configuring “energywise endpoint” on a Cisco 881 router and have PC that is running with Orchestrator Agent.

Workaround: There is no workaround.

- CSCth70437

Symptoms: Crypto sessions drop upon the following error message:

```
000059:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D91910, count=0,
-Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z
000060:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D91CE4, count=0,
-Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z
000061:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D920B8, count=0,
-Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z
000062:%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=83D82F8C, count=0,
-Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz 0x80397B40z
```

Conditions: This symptom is observed on a Cisco 800 series router. In both cases, crypto has been applied to dialer interface.

Workaround: Issue seen previously in CSCta57268.

- CSCth71648

Symptoms: G3 fax fails.

Conditions: This symptom is observed when T38 version 3 is configured on gateway and Cisco fax server.

Workaround: Configure gateway and fax server with T38 version 0.

- CSCth74497

Symptoms: Time elapsed after delay OOP event until route change is more than 3 seconds.

Conditions: This symptom is observed on a router that is loaded with Cisco IOS.

Workaround: There is no workaround.

- CSCth75103

Symptoms: H.323 gateway works call preserve a call when it receives DISCONNECT from ISDN.

Conditions: This symptom is observed when H.323 gateway receives DISCONNECT from ISDN.

Workaround: There is no workaround.

- CSCth75203

Symptoms: Spurious memory access is found while interchanging two configurations.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.1(2.6)T with the two configurations.

Workaround: There is no workaround.

- CSCth78183

Symptoms: Traffic is not transmitted over IPSec tunnel due to duplicate ARP entries and incomplete CEF adjacency.

Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T9.

Workaround: Enter a **shutdown** followed by a **no shutdown** on the tunnel interface.

- CSCth80212

Symptoms: The following topology is seen:

PSTN || (E1) IP Phone---(Sccp)----CUCM(6.1.3)---(Sip trunk)----Gateway --- (Sip trunk)-----Genesys -----Sipclient

Conditions:

1. Calls come from the PSTN to the gateway to the genesys cluster, the sip client behind genesys answers it, the call is fine.
2. Then the call from the PSTN is put on hold and one more call to the IP phone (behind CUCM) is made and that call is also fine.
3. Then there is a transfer (consultative), of the PSTN call to the IP phone.
4. The transferred call is fine for about 30 seconds and then the call drops.

Workaround: There is no workaround.

- CSCth81095

Symptoms: Output queue size is 1000/1000 in the output of “show interface Multilink X”. Also output drops are incrementing on the interface.

Conditions: The complete trigger of the problem is not known yet, but it is related to changing “fair-queue” and “tx-queue-limit” on the member link serial interfaces while bidirectional traffic is flowing over the interfaces.

Workarounds:

1. Enter **shutdown** followed by **no shutdown** on the multilink interface, or flap it from the remote side router
2. Reload the router.

- CSCth82164

Symptoms: When OCSP is being used as the revocation check method for IKE, only the first connection attempt (after reboot or cache clearing of public RSA keys) undergoes an OCSP check. Subsequent revocation checks are bypassed because the peer public key appears to be cached indefinitely.

No CRL or other lifetime parameters are involved. OCSP should be consulted for each IKE tunnel setup.

The following messages indicate bypassing the revocation check:

```
ISAKMP:(1002): peer's pubkey is cached
CRYPTO_PKI: Found public key in hash table. Bypassing certificate validation
```

Conditions: OCSP is configured as revocation check method for IKE.

Workaround: There is no workaround.

- CSCth82293
Symptoms: The Cisco 2900 ISR-G2 router crashes due to bus error at PC 0x0 with spurious errors and %ALIGN-1-FATAL: Corrupted program counter message.
Conditions: This symptom is observed with CNS configurations.
Workaround: There is no workaround.
- CSCth82323
Symptoms: CFD feature fails when onboard crypto engine is enabled on Cisco 1841 platform.
Conditions: This symptom occurs when UUT is running Cisco IOS Release 15.1(2.7.)T.
Workaround: There is no workaround.
- CSCth82777
Symptoms: Router crashes while sending AAA STOP records and cleaning up internal database
Conditions: This symptom may occur when removing a PVC supporting PPP over ATM that is using radius for stop records.
Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(2)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCso20810
Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. Occurs when multicast subsequently flows out a crypto-enabled interface.
Conditions: This bug will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.
Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.
- CSCsv97424
Symptoms: A router will reload due to memory corruption in the I/O pool. As an indication for this bug, we will see the same caller PC in the output of the show buffer pool Serial0/0/0 command.
Conditions: This symptom is observed on Cisco routers that are running the adventerprisek9_ivs-mz feature set and when packets are being processed by an ATM interface.
Workaround: We can overcome the reload issue by disabling hardware crypto using the following command in global configuration mode: **no crypto engine accelerator**.
Further Problem Description: When hardware crypto is turned off, encryption and decryption will be done by software and not by hardware. This can slightly hike CPU utilization, and this should not be an issue as long as we are not hit with pretty huge volume of traffic.
- CSCsz43987
Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.
Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm>

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCsz97091

Symptoms: Packet drop occurs when **show version**, **show run**, and **write memory** commands are issued.

Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.

Workaround: There is no workaround.

- CSCta20040

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm>
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCta58068

Symptoms: During BGP convergence, a CPU spike may be seen on the local PE in an MVPN configuration.

Conditions: The symptom may be observed with the following conditions:

- Remote PE neighbor switchover.
- On local PE, do a **clear ip bgp bgp nbr**
- On bring up of local PE
- Large configurations, such as one with 300 MDT default tunnels.

The following is an example of an MVPN configuration where this problem can be seen:

1. OSPF routing protocol is enabled on all the networks in the topology.
2. Each PE router has 100 mVRFs defined (between vpn_0 to vpn_99).
3. MDT default is configured on all the mVRFs on the PE routers.
4. PE routers have an iBGP session, ONLY with the RR (route-reflector).
5. eBGP session exists between the router and PE1, with router sending 200,010 VPNv4 routes.
6. OSPF session also exists between router and PE1, with router sending 100 OSPF routes.
7. In effect, the following states are present in the network:

On PE and RR routers:

1. IGP states = 100 OSPF routes.
2. BGP states = 200,010 VPNv4 routes.

On PE routers ONLY:

1. VRF sessions = 100 VRFs (vpn0 to vpn_99).
2. MDT sessions = 100 SSM sessions.

Workaround: There is no workaround.

- CSCtb32043

Symptoms: CPUHOG messages may be displayed or Cisco IOS might crash when executing no ipv6 multicast-routing in a configuration with more than 20,000 IPv6 multicast-enabled interfaces or sub-interfaces.

Conditions: This symptom is observed only rarely when an alternate software path is taken. It is not known what causes this alternate path to be taken.

Workaround: There is no workaround.

- CSCtb47647

Symptoms: Active RP crashes at pim_send_join_prune.

Conditions: The symptom is observed when performing some PIM-related testing with specific configurations and after carrying out an SSO. When you attempt to debug memory leak issue using a memory traceback recording command, the router crashes while executing the command **show memory traceback exclusive**.

Workaround: There is no workaround.

- CSCtc42941

Symptoms: Standby is not coming up.

Conditions: When a distribute-list is configured, the ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

Workarounds:

1. When a access list is removed, remove corresponding distribute-list configuration as well.
2. Do not use the same access list name for IPv4 and IPv6.

Further Problem Description:

```
router bgp 100
distribute-list sample in
exit
no ip access-list standard sample
ipv6 access-list sample
permit any any
write mem
```

- CSCtc45177

Symptoms: The “text_start” is not showing up in crashinfo.

Conditions: The symptom is observed with crashinfo data.

Workaround: There is no workaround.

- CSCtc71408

Symptoms: Fax transmission fails when CUBE is in the middle.

Conditions: The symptom is observed when either one of the dial-peers on OGW/TGW/CUBE is configured for fax protocol T38 version 0.

Workaround: Configure version 3 on all dial-peers.

- CSCtc73759

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd30544

Symptoms: NetFlow is showing Null in the destination interface even though packets are not getting dropped or blocked.

Conditions: This symptom is seen when connected to the LNS via VPDN and browsing HTTP. Intermittently Null output is seen as the destination interface as the packet being punted between different CEF switching paths due to **ip tcp adjust-mss value** configuration that is applied on the destination interface.

Workaround: Remove **ip tcp adjust-mss value** from the destination interface.

- CSCtd33567

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte07401

Symptoms: Normal mode GD fails with tracebacks when you execute the **show memory debug leak chunks** command.

Conditions: This symptom is seen when you check for memory leaks after clearing an L2TP session.

Workaround: Wait for all sessions to tear down and then check for leaks.

- CSCte18124

Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024”.

Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.

Workaround: Create ATM PVC without “atm vc-per-vp 1024”.

- CSCte20187

Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (1)
```

The label advertised may be different but it is always a reserved label (0- 15). Additionally, the local PE will see “No Label” as the Outgoing Label” in the MPLS forwarding table.

Conditions: This symptom is observed when bgp next-hop is configured under an interface.

Workaround: There is no workaround.

- CSCte27828

Symptoms: Call forward does not work.

Conditions: Topology: call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider.

IP addresses:

CUCM 10.10.10.3

Cube SUD 10.10.10.2

CUBE North 192.168.101.10

SBC 192.168.100.5

“Call forward no answer” scenario does not work, but not systematically: sometimes it works, sometimes not.

When the “call forward no answer” fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC doesn’t answer due to this.

Workaround: There is no workaround.

- CSCte52369

Symptom: On a Cisco ASR1000 router, the RADIUS will send a NACK for the First COA request message, and Radius Authentication will fail.

Conditions: This symptom is observed when the RADIUS receives “ACCESS-ACCEPT” with ‘Unsupported Vendor’ attribute.

Workaround: Send the COA request message again.

- CSCte53097

Symptoms: When the IP address of the HA is set to the VIP address of HSRP, end-to-end connectivity will be lost. Tunnel keepalives from the mobile node fail and the bindings are deleted from HA.

Conditions: This is seen in Cisco IOS Release 12.4(23) when using the HA behind a NAT device and the translated (inside) IP of the HA is set to the HSRP VIP address.

Workaround: Configure a loopback interface (does not have to be routed) with the same outside (public) IP that the mobile node connects to. This is the outside IP defined in the NAT rule on the NAT device.

- CSCte61495

Symptoms: The following messages are seen with tracebacks:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process = Exec.
```

```
%SYS-2-INTSCHED: 'suspend' at level 3 -Process= "Exec", ipl= 3, pid= 128,
```

Conditions: The symptom is observed when a large ACL is configured for the service-policy. This happens only under ATM subinterfaces.

Workaround: Use small sized ACLs for the service-policy.

- CSCte76092

Symptoms: Cisco 880 series router does not write crashinfo.

Conditions: The symptom is observed with a Cisco 880 series router.

Workaround: Connect a device to monitor the console.

- CSCte82917

Symptoms: On a Cisco 7600 series RSP720, the **show proc cpu sort** command displays a CPU utilization of 0, but the per-process CPU utilization is 100% for some processes; no packet loss occurs, however.

Conditions: This symptom is observed under the following conditions:

- The router has recently loaded
- HSRP is enabled in an HA environment
- A large number of HSRP sessions are established.

Workaround: Reduce the number of HSRP sessions to only a few. The router does not see any performance or functional impact. This is an issue only with internal CPU accounting.

- CSCte92581

Symptoms: A VRF becomes stuck during deletion. This is a rarely-occurring timing condition.

Conditions: This symptom is observed when the **no ip vrf** command is entered.

Workaround: There is no workaround.

Further Problem Description: The stuck VRF cannot be reused.

- CSCte95301

Symptoms: Memory leak in proxy authentication scenario, when authentication fails.

Conditions: The symptom is observed when HTTP proxy authentication is used.

Workaround: There is no workaround.

- CSCte98082

Symptoms: PPPoE session is not coming up on some clients due to a malformed PADO. PPPoE relay sessions are failing to come up on an LAC.

Conditions: The symptom is observed with a few clients which are unable to process malformed PADO and also when “pppoe relay service” is configured on the LAC.

Workaround: There is no workaround.

- CSCtf01344

Symptoms: IOSD core@chunk_diagnose while doing an ISSU on a Cisco ASR 1004 router.

Conditions: The symptom is observed on a Cisco ASR 1004 when attempting an ISSU upgrade with VRF-aware IPsec features and an uninitialized Webex SPA in the system.

Workaround: Properly initialize Webex SPA before ISSU.

- CSCtf17624

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each

advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf35006

Symptoms: If there are two jobs in an SNMP job queue and if you try to destroy the jobs, the console hangs.

Conditions: The symptom is observed if you prepare multiple license action entries and then let them execute immediately.

Workaround: There is no workaround.

- CSCtf48094

Symptoms: UUT crashes for FTP traffic with debugs enabled for IPv6 inspection.

Conditions: The symptom is observed only with Legacy Firewall for IPv6 inspection.

Workaround: There is no workaround.

- CSCtf72678

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm>

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCtf91428

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat>

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf98087

Symptoms: A Cisco router reloads at sipSPIUpdSrtpSession.

Conditions: This symptom is observed after completion of the basic call with a hold/resume scenario with IPv6 mode.

Workaround: There is no workaround.

- CSCtg14446

Symptoms: Packets are dropped in excess of the configured rate for hierarchical policies, with shaper in the parent policy.

Conditions: The symptom is observed only with HQoS policies (flat policies are not affected).

Workaround: There is no workaround.

- CSCtg21685

Cisco IOS Software contains a vulnerability when the Cisco IOS SSL VPN feature is configured with an HTTP redirect. Exploitation could allow a remote, unauthenticated user to cause a memory leak on the affected devices, that could result in a memory exhaustion condition that may cause device reloads, the inability to service new TCP connections, and other denial of service (DoS) conditions.

Cisco has released free software updates that address this vulnerability. There is a workaround to mitigate this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sslvpn>.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

<http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle>

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtg30795

Symptoms: Calls are not torn down since SIP INFO with Qsig disconnect tunneled are not honored by the SIP gateway.

Conditions: This symptom is observed when disconnect is built and sent by Call manager over a Qsig-enabled SIP trunk to the SIP gateway (GW).

CUCM1---SIP-QSIG-----SIP GW-----T1 QSIG-----MGCPGW-----CUCM2

In the above setup, when CUCM1 initiates disconnect, it sends out INFO tunneled with Qsig disconnect to the SIP GW in order to achieve 3-way disconnect.

Workaround: There is no workaround.

Further Problem Description: The gateway should send a Qsig Disconnect over the T1 link; since that is not happening, the call is not torn down.

- CSCtg31434

Symptoms: A Cisco router crashes due to an unexpected exception to the CPU.

Conditions: This symptom occurs when the **privilege interface level 10 ppp authentication** command is entered. This symptom is observed in Cisco IOS Release 12.2(31)SB through Release 12.2(31)SB18, and in Cisco IOS Releases 12.2(33)SB and 12.2(34)SB.

Workaround: There is no workaround.

- CSCtg35230

Symptom: VPDN sessions are created when SCCRQ and SCCRP have different IP addresses.

Conditions: This symptom occurs after the IP address is downloaded from the AAA server and changed on LNS2.

Workaround: There is no workaround.

- CSCtg41733

Symptoms: Certain crafted packets may cause memory leak on a Cisco IOS router.

Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.

Workaround: Disable SIP if it is not needed.

- CSCtg51476

Symptoms: Cisco ISR G2 routers reload on their own with a bus error.

Conditions: This symptom is observed when BFD is configured.

Workaround: Remove BFD.

- CSCtg56013

Symptoms: Router crashes when initiating ping through the modem after router bootup.

Conditions: The symptom is observed when the modem fails to enumerate at bootup.

Workaround: There is no workaround.

- CSCtg59956

Symptoms: Active supervisor crashes when doing an SSO switchover.

Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

Workaround: There is no workaround.

- CSCtg67425

Symptoms: A Cisco router crashes at `fr_vcb_dldci_status_change`.

Conditions: This symptom is observed after removing frame-relay encapsulation in a router that has T3 interfaces.

Workaround: Remove all the pvc's configured under an interface before changing/removing frame-relay encapsulation.

- CSCtg69202

Symptoms: CUBE modifies the RTP port number before passing it to the remote end, which causes one-way audio.

Conditions: This symptom is observed only when the RTP port number is higher than the RTCP port number in the incoming request from the endpoint. Instead of sending the same RTP port number, CUBE decrements the RTP port number by one less than the RTCP port number when it forwards the OLC Ack to the destination side. This causes the destination to send the audio packets to the wrong port on the originating side, causing one-way audio.

Workaround: There is no workaround.

Further Problem Description: Under some specific conditions, when CUBE receives the OLC acknowledgement with the media control information from an H323 client, instead of passing the same RTP port number to the remote end, it modifies the RTP port number, causing the one-way audio.

- CSCtg76688

Symptoms: An active Cisco route processor reloads in a scale scenario (16k - 24k sessions) when the **clear subscriber session all** command is entered.

Conditions: This symptom is observed only when there are 16k-24k sessions and the **clear subscriber session all** command is entered.

Workaround: Do not enter the **clear subscriber session all** command when more than 16k sessions are up on the router.

- CSCtg79105

Symptoms: A UC560 unexpectedly reboots.

Conditions: The symptom is observed when the **show memory 0** command is executed.

Workaround: There is no workaround.

- CSCtg83932

Symptoms: "Encapsulation aal5auto" may not be enabled under svc mode.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(01.14)T.

Workaround: There is no workaround.

- CSCtg86714

Symptoms: The **show cellular 0** command might not show any output.

Conditions: The symptom is observed with the **show cellular 0** command.

Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the “MODEM UP” line, you get “LINK UP” and still retain the **show cellular stats**.

- CSCtg87775

Symptoms: The router may unexpectedly reload.

Conditions: The symptom is observed under circumstances where a Cisco 7600 series router is configured to handle several hundred or more neighbors, and an administrator issues the command: **clear bgp vpv4 unicast ***.

Workaround: Clear individual neighbors separately, limiting yourself to 100 or fewer in any scanner interval.

Further Problem Description: Issuing other clear commands and forcing a switchover between active and standby at during the interval immediately before and after issuing the **BGP clear** command increases the probability of a reload.

The number of neighbors where this is documented as happening is 1200, but the exact minimum number of neighbors needed to trigger the problem is not documented.

- CSCtg88766

Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

Workaround: There is no workaround.

- CSCtg91201

Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

Workaround: There is no workaround.

- CSCtg91336

Symptoms: A Cisco router may crash during show command **show ip ospf rib**.

Conditions: This symptom is observed on Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

- A user enters the **show ip ospf rib** command and stops in the middle
- OSPF local rib is significantly changed; for example, routes are removed
- A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

Workaround: Do not enter the **show ip ospf rib** command. If it is necessary use the command, enter terminal length 0 and print the entire output.

- CSCtg95618

Symptoms: 1. MSCD_StartStop fail message is observed in usbflash_mscd_scsi_listener 2. USB flash file system is not accessible sometimes.

Conditions: This symptom is observed on Cisco 892F and C892FW series routers with two USB slots when the USB sticks are removed and swapped. This symptom is not observed when a single USB stick is removed or inserted in a different bus.

Workaround: There is no workaround.

- CSCtg96518
Symptoms: Fast memory leak occurs in CCSIP CCB Pool.
Conditions: This symptom is observed on a Cisco 2951 integrated services router with Cisco IOS Release 15.1(1)T.
Workaround: Reload the router.
- CSCtg96630
Symptoms: A Cisco router crashes when the user tries to configure a default policy with rsvp group percentage configuration.
Conditions: This symptom is observed when the user tries to configure a default policy with rsvp group percentage configuration under a virtual template.
Workaround: There is no workaround except to avoid this configuration command.
- CSCtg98783
Symptoms: Cube: call leg 1 receives SDP 101, 0-15; Cube: call leg 2 sends SDP 101, 0-16. This is seen as a different media, and is treated as such.
Conditions: This symptom is observed when Cube is configured in DO-EO with flow-around.
Workaround: There is no workaround.
- CSCtg99114
Symptoms: The following error message with traceback is observed:

```
%IPC-5-REGPORTFAIL: Registering Control Port
```


Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.
Workaround: Drop IPC traffic using control-plane policing:

```
class-map match-all ipc match access-group name ipc policy-map drop-ipc class ipc drop
ip access-list extended ipc permit udp any any eq 1975 control-plane service-policy
input drop-ipc
```
- CSCth01939
Symptoms: IPSEC packets are dropped on the router and an error is displayed on the console.
Conditions: This symptom is observed on a Cisco IAD2430 with VPN/GRE tunnel configuration and AES256 encryption.
Workaround: There is no workaround.
- CSCth02725
Symptoms: There is an interoperability issue between a third-party vendor's routers and Cisco routers with severe IPTV service failure in Prune-Overriding environment.
Conditions: The symptom is observed in the following scenario:
 1. Router A is Cisco 7609 router (IP address 10.1.1.1) and connects to Router B (third-party vendor's router; IP address 10.1.1.3) and Router C (IP address 10.1.1.2).
 2. If subscriber under Router C disappears, Router A receives "Prune" message from Router C.
 3. Router A does not change "source IP of PruneEcho message (10.1.1.2)" and sends it to Router B.
 4. At this time, Router B should send overriding-join to Router A because Router B still has subscribers. But Router B drops the PruneEcho message because source IP (10.1.1.2) is not from PIM neighbor. Router B cannot send overriding-join to Router A.

- 5. As a result, multicast traffic (IPTV stream) to Router B stops.

Workaround: Connect C and B to become PIM neighbors avoids the interoperability issue, but cannot always be considered a recommended workaround because of potential high cost and/or other (sometimes third-party) limitations.

- CSCth02789

Symptoms: System can crash when attempting to schedule an IPv6 icmp-echo operation.

Conditions: The symptom is observed with IPv6 and icmp-echo.

Workaround: There is no workaround.

- CSCth04193

Symptoms: A Cisco router crashes at cce_dp_named_db_http_free_token_info.

Conditions: This symptom is observed when Zone-based Policy Firewall is configured to inspect HTTP traffic.

Workaround: Do not use deep packet inspection.

- CSCth04945

Symptoms: A Cisco router crashes when adding or removing a QoS policy from an interface.

Conditions: This symptom is observed when the following occur:

- packets keep hitting the interface from which the policy is being removed
- the QoS policy is at least a two-level policy -before the policy was removed, the CLI generated an error for some invalid configuration change in that policy; for example,

```
3845-AA2205(config)
#policy-map VOICE-OUT-PARENT 3845-AA2205(config-pmap)
#class class-default 3845-AA2205(config-pmap-c)
#no shape average 100000000
```

Queueing must be removed from child classes before queueing can be removed from class-default.

Workaround: Avoid invalid configuration changes in the QoS policy before adding it to or removing it from an interface.

- CSCth07787

Symptoms: A standby device crashes when attempting to configure login banner on the active device.

Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters: -Cntrl-v + Cntrl-C; -Shift-6 + Shift-C

Workaround: Use any delimiters other than the following: -Cntrl-v + Cntrl-C; -Shift-6 + Shift-C.

- CSCth08505

Symptoms: PPPoE sessions may not sync to the standby-RP.

Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

Workaround: Reloading the standby-RP may resolve this issue.

- CSCth15353

Symptoms: Incorrect result codes are displayed in vpdn sys logging. The CDN message for admin down was reported in the syslog as "Result Code=2, Error Code=6" instead of "Result Code=3, Error Code=6".

Conditions: This symptom is observed when a session is cleared by a clear command (for example, **clear interface virtual-access 3.1**).

Workaround: There is no workaround.

- CSCth15518

Symptoms: Ping through ISDN BRI interface fails.

Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.

Workaround: There is no workaround.

- CSCth16382

Symptoms: A Cisco device crashes at `cce_dp_results_get_class_group_element`.

Conditions: This symptom is observed when Crypto is on and QoS pre-classify is not enabled. The crash occurs when configurations are loaded and traffic is run.

Workaround: There is no workaround.

- CSCth18146

Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

Workaround: There is no workaround.

- CSCth18611

Symptoms: A Cisco router crashes.

Conditions: This symptom is observed when configuring dynamic nat under the vrf interface with an existing firewall configuration. This symptom is not observed without the vrf configuration.

Workaround: There is no workaround.

- CSCth18982

Symptoms: BGP sessions flap continuously in a multi-session configuration.

Conditions: This symptom is observed when the same peer under the same address family is configured under different topologies (MTR with GR-enabled setup) with multiple topo-ids.

Workaround: The sessions do not flap if topologies use the same topo-id for the peers active under different topologies or when GR is not enabled.

- CSCth20704

Symptoms: A Cisco router crashes when policy-map is unconfigured while traffic is flowing.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T1.

Workaround: There is no workaround.

- CSCth21017

Symptoms: Traceback is seen when ISIS adjacency state changes.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS 15.1(1)T1.

Workaround: There is no workaround.

- CSCth23787

Symptom: A Cisco router crashes at `mcast_aaa_send_stop_acct_event`.

Conditions: This symptom is observed while unconfiguring “ipv6 mld join-group FF1E:7777:7777:1” in the client after configuring within 15-20 seconds.

Workaround: Unconfigure, if required, after multicast start record is sent.

- CSCth23814

Symptoms: When using Flexible NetFlow, a traceback or crash can occur.

Conditions: This symptom is observed when a monitor is configured with a flow record that has the “BGP next hop” field configured.

Workaround: Ensure that the “BGP next hop” field is not configured for a flow.

- CSCth25698

Symptoms: IPv6 packets are not dropped by the firewall.

Conditions: IPv6 packets are not dropped by the firewall in case of Zone to non-zone.

Workaround: There is no workaround.

- CSCth28677

Symptoms: CUD fails to be parsed when it contains 0x00.

Conditions: This symptom is observed on a Cisco router configured for X25 translation with CUD verification.

Workaround: There is no workaround.

- CSCth29105

Symptoms: On Cisco ISR G2 products—only on the Cisco 2901, 2911, and 2921—occasionally the SYSTEM LED will be OFF even when the router is operating normally.

Conditions: There are no specific conditions that trigger this issue. The problem happens randomly.

Workaround: There is no workaround. This issue does not affect any of the router functionality.

- CSCth30815

Symptoms: StopCCN result codes and strings do not match RFC.

Conditions: This symptom is observed when the session is cleared by command or due to some error condition; the result code is not correct.

Workaround: There is no workaround.

- CSCth33457

Symptoms: A Cisco IOS router configured with IPSec (IP Security) may reload when receiving encrypted packets.

Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

- ip accounting precedence input
- ip accounting mac-address input
- WCCP
- Flexible NetFlow
- BGP accounting
- uRPF
- mpls accounting experimental input

Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth35377

Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

Conditions: This symptom is observed on a Gigabit Ethernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters:

```
encapsulation dot1Q xxx ip pim sparse-mode.
```

Workaround: Remove “ip pim sparse-mode.”

- CSCth35620

Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

Conditions: The symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

Workaround: There is no workaround.

- CSCth35780

Symptoms: A Cisco router crashes for the SIP multi-part traffic.

Conditions: This symptom is observed when SIP multi-part traffic passes through a Cisco 7200 router. NAT SIP Multi-part must be enabled as part of the NAT configuration.

Workaround: There is no workaround.

- CSCth38711

Symptoms: The first WAAS connection takes longer than one minute to begin transferring data.

Conditions: This symptom is observed during AOIM sync, which occurs once per boot or reconfiguration.

Workaround: There is no workaround.

- CSCth39774

Symptoms: UUT hangs when an eTCDF file is loaded on the router in the latest t_base_1 code base.

Conditions: The symptom is observed when an eTCDF file is loaded on the router, the UUT seems to hang. However, the UUT is actually waiting for user input, and if you enter “#” on the CLI, it will print some error messages about invalid commands and return to CLI.

Workaround: Do not use the eTCDF file to configure the encrypted filter, rather directly enter the commands on the CLI of the router.

- CSCth39877

Symptoms: No VPDN logging occurs for the L2TP tunnel.

Conditions: This symptom is observed when the tunnel goes down.

Workaround: There is no workaround.

- CSCth40090

Symptoms: A Cisco device crashes when initiating an analog CAMA call.

Conditions: On initiation of an analog CAMA call, a crash occurs due to memory corruption leading to a breakpoint exception. A crash occurs in scenarios where e911 is enabled or disabled.

Workaround: There is no workaround.

- CSCth40213

Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

Workaround: There is no workaround.

- CSCth40506

Symptom: A Cisco voice gateway does not have its Gigabit Ethernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

```
-- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
```

Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

```
-- .May 4 17:49:29.120 GMT=+1: ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry:
Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
```

The call, however, is not cleared from the PRI.

- CSCth45623

Symptoms: A memory leak occurs in cce dp reclass.

Conditions: This symptom is observed with WAAS Express plus QoS preclassify disabled plus Crypto plus crypto-map.

Workaround: There is no workaround.

- CSCth50550

Symptoms: A Cisco device crashes when using PDP filter.

Conditions: This symptom is observed when PDP filter is applied in a QoS Policy.

Workaround: There is no workaround.

- CSCth51125

Symptoms: PCEX-3G-HSPA-R6 is not recognized at bootup:

```
%CISCO800-2-MODEM_NOT_RECOGNIZED: Cellular0 modem not RECOGNIZED. Carrier id not
available or invalid! Replace it with Cisco supported modem and reload the router.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
```

Conditions: The symptom is observed on a Cisco 881G-K9 that is running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCth57478

Symptoms: When configuring SIP digest authentication, user names with more than 25 characters are truncated in the running config and cause the password component to be corrupted. This error is saved through to startup configuration, causing the authentication to be lost on reboot.

Conditions: This symptom is observed with a normal dial-peer configuration on a POTS dial-peer running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCth59217
Symptoms: Firewall sessions are not seen when ZBFW and gatekeeper are configured on the UUT.
Conditions: The symptom is observed when ZBFW and gatekeeper are configured on the UUT.
Workaround: There is no workaround.
- CSCth62854
Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.
Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.
Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.
- CSCth63379
Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.
Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.
Workaround: There is no workaround.
- CSCth69243
Symptoms: Error messages and tracebacks involving the TCP timer process appear on the console.
Conditions: This symptom is observed with a large volume of traffic over extended periods of time; the exact trigger is unknown.
Workaround: There is no workaround.
- CSCth79434
Symptoms: Policies with mixed filters might not work properly.
Conditions: If a policy has a filter of type dscp/prec/acl in its first class- map, the rest of the policy might not classify properly.
Workaround: If the policy has non-dscp/prec/acl filters in it, moving that class-map to the top of the policy will alleviate this problem.



Caveats for Cisco IOS Release 15.1(3)T

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- [Resolved Caveats—Cisco IOS Release 15.1\(3\)T4, page 412](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(3\)T3, page 420](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(3\)T2, page 441](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(3\)T1, page 465](#)
- [Open Caveats—Cisco IOS Release 15.1\(3\)T, page 489](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(3\)T, page 521](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Resolved Caveats—Cisco IOS Release 15.1(3)T4

Cisco IOS Release 15.1(3)T4 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T3 but may be open in previous Cisco IOS releases.

- CSCsv30540

Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and a traceback are seen.

Conditions: This symptom is observed when the **show running-config/write memory** command is issued.

Workaround: There is no workaround.

- CSCtj48387

Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP related errors.

Conditions: This symptom occurs when DHCP is enabled and sessions get DHCP information from a RADIUS server.

Workaround: There is no workaround.

- CSCtn65116

Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

Conditions: This symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Cisco IOS Release 12.2(33)SRB or later releases. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, for example, 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). This issue is seen with the following process:

1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
2. The allocated label changes from 16 to 17, for example, due to interface flapping or BGP attribute change.
3. However, before the BGP import happens, a more specific prefix (for example, 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, the RT policy.

Workaround: Remove the RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCtq24557

Symptoms: The router crashes after deleting multiple VRFs. This happens very rarely.

Conditions: This symptom is observed in a large scale scenario.

Workaround: There is no workaround.

- CSCtq59923

Symptoms: OSPF routes in RIB point to an interface that is down/down.

Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

Workaround: Configure “ip routing protocol purge interface”.

- CSCtq78217

Symptoms: A router crashes with the following information:

System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ

Conditions: This symptom is observed with CUBE + SIP.

Workaround: There is no workaround.

- CSCtr86328

Symptoms: A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.

Conditions: This symptom is observed when a Cisco IOS device is configured for clientless SSL VPN.

Workaround: There is no workaround.

Further Problem Description: This problem has been seen when the stock Andorid browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C>

CVE ID CVE-2012-1344 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr88739

Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: These symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove "import-route target" and reconfigure route-target.

Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCts70790

Symptoms: A Cisco 7600 router ceases to advertise a default route configured via "neighbor default-originate" to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

Workaround: Remove and readd the **neighbor default-originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCtt02313

Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code is integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

Workaround: There is no workaround.

- CSCtt26721

Symptoms: A Cisco router may see increased CPU utilization when NBAR is used.

Conditions: This has been experienced on a Cisco 3925 router running Cisco IOS Release 15.1(3)T2.

Workaround: There is no workaround.

- CSCtt94391

Symptoms: A Cisco wireless router may unexpectedly reboot due to a bus error with the following error leading up to the crash:

```
ASSERTION FAILED: file '../dot11t/t_if_dot11_hal_ath.c'', line XXXX
```

Conditions: This symptom relates to the wireless on the router. This crash can be seen on the following platforms: Cisco 870W, Cisco 1800W, Cisco UC500W, and Cisco 2800 and Cisco 3800 routers with HWIC-AP. The crash is only seen when an iPhone 4S is connected to the router. The crash has most commonly been triggered by running a video call application on the phone, but there may be other triggers. Other than the wireless configuration and other generic configurations needed to provide connectivity to the router, no other specific configuration is needed to see the crash.

Workaround: There is no workaround on the router. However, this issue is not seen with an iPhone 4s running iOS 5.1. The issue is only seen on iOS 5.0.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C>

CVE ID CVE-2012-1327 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtu18786

Symptoms: A device may crash showing “VOIP” error messages. Decodes point to voice functions.

Conditions: This symptom is observed when SIP is enabled on the device.

Workaround: There is no workaround.

- CSCtu36224

Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.

Workaround: There is no workaround.

- CSCtw45055

Symptoms: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault, if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from
session Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from
session Neighbor deleted
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
```

```
Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC
```

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
```

The scheduler process will attempt to reference a freed data structure, causing the system to crash.

Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

Workaround: There is no workaround.

- CSCtw59086

Symptoms: Connecting via Cisco AnyConnect or the WebVPN portal on a Cisco IOS router fails. The following message is seen in the Syslog:

```
%SSLVPN-6-LICENSE_NO_FREE_COUNT: All available SSLVPN session licenses are in use
```

Conditions: This symptom is observed when the WebVPN License counter incorrectly reads 4294967295. Also, no connections are visible while executing the **show webvpn session context all** command.

For example:

```
sh webvpn session context all
show webvpn license
Max platform license count : 1500
Available license count      : 100
Reserved license count       : 100
* In-use count                : 4294967295*
```

Workaround: Reload the Cisco router.

- CSCtw76527

Symptoms: The crypto session stays in UP-NO-IKE state.

Conditions: This symptom occurs when using EzVPN.

Workaround: There is no workaround.

- CSCtw98456

Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK, but no traffic is going out over the tunnel.

Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

For example, the IVRF routing table should show:

```
S          10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
```

but instead it shows:

```
S          10.0.0.0 [1/0] via 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99290

Symptoms: The source or destination group-address gets replaced by another valid group-address.

Conditions: This symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

Workaround: There is no workaround.

- CSCtx29543

Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when issuing the **show ip route** command.

Conditions: This symptom occurs under the following conditions:

1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exists.
2. A default route exists.
3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

The router may now crash when issuing the **show ip route** command or when the default route is updated.

Workaround: There are two possible workarounds:

1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
2. If workaround #1 is not possible, then ensure that at least one supernet route for all possible mask lengths exists at all times, for example, by configuring summary routes that do not interfere with normal operation.

- CSCtx32628

Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

- BGP full mesh is configured.
- BGP cluster-id is configured.
- **address family vpnv4** is enabled.
- **address family ipv4 mdt** is enabled.
- The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

Workaround: Remove the cluster-id configuration or hard-reset the BGP session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx38806

Symptoms: SSL VPN users lose connectivity as soon as a Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

The problem affects Firefox also (version 10.0.1), displaying the following message:

“The page isn’t redirecting properly”

Conditions: This symptom is observed on Cisco IOS that is acting as a headend for SSL VPN connections.

Workaround: Any of the following workarounds will work:

1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
2. Uninstall the update.
3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

```
webvpn gateway gateway name
  ssl encryption rc4-md5
```

4. Use AC 2.5.3046 or 3.0.3054.
5. Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:

“Connection attempt has failed due to server communication errors. Please retry the connection”

The AnyConnect event log will show the following error message snippet:

```
Function: ConnectIfc::connect Invoked
Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx77750

Symptoms: Crosstalk may be heard by PSTN callers when a call is placed on hold and Music on Hold (MMOH) is enabled.

Conditions: This symptom is observed when CUCM is configured to do Multicast MoH.

Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS or use SIP Multicast MoH.

Workaround 2: Use Unicast MoH.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:ND/RC:C>

CVE ID CVE-2012-1361 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx88093

Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.

Conditions: This symptom occurs while using the **dialer-list x protocol ip deny** command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.

Workaround: Use the method that follows to define interesting traffic instead of the **dialer-list x protocol ip deny** command:

```
access-list x protocol ip deny
dialer-list 1 protocol ip list x
```

- CSCty43587

Symptoms: Crash observed with memory corruption similar to the following:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc
XXXXXXXX, dealloc XXXXXXXX
```

Conditions: This symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

Workaround: There is no workaround.

- CSCty77190

Symptoms: DTLS is switched back to TLS after reconnect.

Conditions: This symptom is observed with the following conditions:

- Test image: c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
- Test version: Cisco IOS Release 15.2(01)T

Workaround: Restart the AnyConnect client.

- CSCty80074

Symptoms: A Cisco 3800 router running Cisco IOS Release 15.0(1)m7, with only Multilink or Serials, shows aborts and input errors during normal traffic conditions.

Conditions: This symptom is observed with normal traffic load. In addition, when a ping sweep is done, aborts and input errors are seen more frequently.

Workaround: There is no workaround.

- CSCty83520

Symptoms: IP Phone -- CUCM --- H323 -- 3845 - PSTN

1. A call is originated from the IP phone to a PSTN number and it gets connected.
2. The IP phone puts the call on hold.
3. The CUCM instructs GW to listen to the Multicast MoH stream.
4. The Cisco IOS Gateway sends the RTCP packet to Multicast MoH.

Conditions: This symptom is observed when the H.323 Gateway is configured and the Multicast MoH and MoH stream is sent across an IP Multicast network.

Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS.

Workaround 2: Use Unicast MoH.

- CSCtz27137

Symptoms: An upgrade to the S640 signature package may cause a Cisco IOS router to crash.

Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:

- Cisco IOS Release 12.4(24)T4
- Cisco IOS Release 15.0(1)M4
- Cisco IOS Release 15.0(1)M8
- Cisco IOS Release 15.2(3)T

Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:

- Access the router via the console.
- Enter break sequence to access ROMmon mode.
- Change the config-register value to 0x2412.
- Boot the router to bypass the startup-configuration.
- Configure the basic IP parameters.
- TFTP a modified configuration to the router's running-configuration with Cisco IOS IPS disabled.
- Reset the config-register to 0x2102.
- Enter the **write memory** command and reload.

Resolved Caveats—Cisco IOS Release 15.1(3)T3

Cisco IOS Release 15.1(3)T3 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T3 but may be open in previous Cisco IOS releases.

- CSCsh39289

Symptoms: A router may crash under a certain specific set of events.

Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCso41274

Symptoms: A router crashes or shows the following traceback:

```
% Not enough DSP resources available to configure ds0-group 1 on controller T1 1/0 %
The remaining dsp resources are enough for 14 time slots. % For current codec
complexity, 1 extra dsp(s) are required to create this voice port.
sip-cme(config-controller)# %ALIGN-3-SPURIOUS: Spurious memory access made at
0x40C627A8 reading 0x4 %ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C
0x40D72E74 0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
```

Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

Example:

```
sip-cme(config)# controller t1 1/0
sip-cme(config-controller)# ds0-gr 1 time 1-16 type e&m-imm
sip-cme(config-controller)# ds0-gr 1 time 1-16 type e&m-immediate-start
```

Workaround: Ensure that there are more DSPs in the router than signalling channels.

- CSCta11223

Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

Conditions: This symptom is observed when the device is running Cisco IOS software and is configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

Workaround: There is no known workaround.

- CSCtb72734

Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

Workaround: There is no workaround.

- CSCtd15853

Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

Conditions:

- mVPN is configured on the PE router.
- Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

Workaround: There is no workaround.

- CSCtg67346

Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show “Di1 DDR: dialer_fsm_pending() di1”.

Conditions: The conditions are unknown at this time.

Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCtg68047

Symptoms: The router reloads.

Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

Workaround: Wait until the tunnels are shut down before issuing the show command.

- CSCth14305

Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if link members flap because the changes in bandwidth will not be handled correctly.

Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth20018

Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, **no interface g0/0.100** or **no interface atm0/0.100**) may sometimes crash the system.

Conditions: This symptom occurs during basic configuration.

Workaround: Do not unconfigure a subinterface.

- CSCth73173

Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCth90147

Symptoms: Router will respond to an RS with an RA.

Conditions: The symptom is observed when you configure the **ipv6 nd ra suppress** command. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

Workaround: Use an ACL to block the reception of RS packets.

- CSCti01036
Symptoms: A Cisco ASR 1000 series router crashes on the RADIUS process.
Conditions: This symptom is observed on a Cisco ASR 1000 series router with RADIUS AAA services enabled. When the RADIUS server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.
Workaround: Prevent the AAA server from sending empty VSA strings.
- CSCti04919
Symptoms: While unconfiguring and reconfiguring the VRF, PIM neighborship goes down in a specific scenario.
Conditions: This symptom occurs if the PIM MDT GRE tunnel takes more time to come up compared to other interfaces in the VRF.
Workaround: Toggle the default MDT.
- CSCti33159
Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.
Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.
Workaround: There is no workaround.
- CSCti64685
Symptoms: User may not be able to configure SLA MPLS configuration.
Conditions: This symptom occurs when the router is booted up and may be random.
Workaround: There is no workaround.
- CSCtj21237
Symptoms: “%SYS-2-LINKED: Bad enqueue, Bad dequeue” messages are received, which might result in an unexpected reboot due to SegV Exception.
Conditions: The symptom is observed on a router configured with control plane policing and protection feature.
Workaround: Disable the feature in order to prevent any further crash.
- CSCtj46670
Symptoms: IPCP cannot complete after dialer interface is moved out of Standby mode. CONFREJ is seen while negotiating IPCP.
Conditions: The symptom is observed when a dialer interface has moved out from standby mode.
Workaround: Reload the router.
- CSCtj56551
Symptoms: The Cisco 7600 crashes in a very rare case.
Conditions: This symptom is observed very rarely when route-churn/sessions come up.
Workaround: There is no workaround.
- CSCtj79769
Symptoms: LC crashes.
Conditions: When disabling MLD snooping on an interface or disabling IPV6 multicast in general.

- Workaround: There is no workaround.
- CSCtj95685

Symptoms: A router configured as a voice gateway may crash while processing calls.

Conditions: The symptom is observed with a router configured as a voice gateway.

Workaround: There is no workaround.
 - CSCtj96915

Symptoms: An LNS router hangs up at the interrupt level and goes into an infinite loop.

Conditions: Unknown. See Further Problem Description below.

Workaround: There is no workaround. Only a power-cycle can remove the symptom.

Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe that this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.
 - CSCtk00181

Symptoms: Password aging with crypto configuration fails.

Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

Workaround: There is no workaround.
 - CSCtk01638

Symptoms: Analog endpoint and connection trunk is torn down due to the following Q.850 cause code in SIP BYE request:

Port will show in a S_TRUNK_PEND

```
*****
show voice call summary | include 0/2/0
0/2/0 - - - S_TRUNK_PEND
```

Conditions: This symptom is observed when the **clear counters** command is invoked. This triggers the gateway to stop sending rtcp events, which causes media inactivity to be activated on the far-end gateway and the connected trunk to be torn down.

Workaround: There is no workaround.
 - CSCtk32975

Symptoms: The system crashes.

Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

Workaround: There is no workaround.
 - CSCtk74685

Symptoms: When H225 messages for a call are sent out to the wrong TCP socket by a Cisco IOS gateway, they may sent to a completely different IP than the one that is aware of the call. When this occurs, the new socket gets paired to the call and the H323 stack tries to tear down the H245 socket for a call that is being disconnected. Instead, it erroneously tears down an unrelated calls H225 socket. This causes the unrelated call to drop.

Observed with debug cch323 all and debug ip tcp trans:

```

13090333: Dec 3 13:18:20.965: //137091/80C6B1F78F31/H323/run_h245_iwf_sm: received
IWF_EV_H245_DISCONN while at state IWF_ACTIVE 13090334: Dec 3 13:18:20.965:
//137091/80C6B1F78F31/H323/cch323_send_event_to_h245_connection_sm: Changing to new
event H245_DISCONNECT_EVENT 13090335: Dec 3 13:18:20.965:
//137091/80C6B1F78F31/H323/cch323_h245_connection_sm: state=0, event=4,
ccb=C5E442B8, listen state=2 13090336: Dec 3 13:18:20.965:
//137091/80C6B1F78F31/H323/cch323_h245_connection_sm: H245_CONNECT: Received event
H245_DISCONNECT_EVENT while at H245_NONE state 13090337: Dec 3 13:18:20.965: TCP0:
state was ESTAB -> FINWAIT1 [24696 -> 192.0.2.100(1720)] 13090338: Dec 3 13:18:20.965:
TCP0: sending FIN

```

Conditions: This symptom occurs with all Cisco IOS images with the fix for CSCin76666.

The cascade issue noted in this bug is triggered by an event where CM closes down an H225 or H245 TCP socket mid-call. Due to the cascading nature of CSCtk74685, identifying the root call that triggers this socket conflict may be extremely difficult, until the fix for CSCtk74685 is applied.

Workaround: Use one of the following workarounds:

1. Enable call preservation on CM, which does not prevent the socket from getting torn down, but minimizes user impact and does not drop audio on the call.

voice service voip h323 call preserve

System > Service Parameters > (Select Publisher Node) > Cisco CallManager > Advanced > Allow Peer to Preserve H.323 Calls > False > Save

2. Run a Cisco IOS release that does not have the fix for CSCin76666.

3. Change the signaling protocol to SIP.

- CSCtl52854

Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

Conditions: The symptom is observed when a multicast server is connected to an EHWIC L2 interface.

Workaround: Connect the multicast server to an on-board gig interface.

- CSCtl90341

Symptoms: A router crashes due to an NHRP stack overflow.

Conditions: This symptom occurs very inconsistently.

Workaround: There is no workaround.

- CSCtn04357

Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

vlan configuration 161

ip flow monitor flowmonitor1 in

ip flow monitor flowmonitor1 input

Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

Workaround 1: Remove the flow monitor configuration.

Workaround 2: Use netflow-v9 export protocol.

Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn16855

Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn22728

Symptoms: See the following:

```
Router(config)# monitor session 1 type erspan-source
Router(config-mon-erspan-src)# destination ?
<cr>
Router(config-mon-erspan-src)# destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on command:
    destination int g11/48
due to parser return error
```

Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

Workaround: Do not issue not applicable commands.

- CSCtn32323

Symptoms: 802.1p information is not set on local generated traffic when bridge-dot1q is used on the DSL lines.

Conditions: Configure the device to transport 802.1p information over a DSL link connection, considering different CoS values for LAN and local generated traffic on the router.

```
interface ATM0.y point-to-point
  bridge-group <x>
  pvc 1/199
    bridge-dot1q encap <vlan>
    service-policy out <egress-policy>
```

Workaround: There is no workaround.

- CSCtn62287

Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

Workaround: There is no workaround.

- CSCtn68643

Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption.

**ipv6 ospf encryption ipsec spi 500 esp null sha1
12341234123412341234123412341234123412341234**

or

ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd

Workaround: There is no workaround.

- CSCtn74169

Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process

Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept.

Workaround: Do not use long banner in HTTP intercept.

- CSCtn74673

Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.

Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** command does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.

Workaround: There is no workaround other than line card reload.

- CSCtn83520

Symptoms: VOIP_RTCP related traceback is seen.

Conditions: This symptom is observed when IPIP gateways are involved.

Workaround: There is no workaround.

- CSCto08135

Symptoms: When a deny statement is added as the first ACL, the message gets dropped.

Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.

Workaround: Turn off the VSA, and go back to software encryption.

- CSCto14435

Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto15371

Symptoms: A router may unexpectedly reload due to a bus error.

Conditions: This symptom occurs only when two peers are configured in crypto map and the first peer is unreachable.

Workaround: Do not use two “set peer” statements in the crypto map definition.

Further Problem Description:

- 1) Configure 880 to use the software crypto engine.
- 2) Apply the exact configuration of the UUT to 880. The critical factor is the unreachable peer, which needs to appear before the connected peer.

```
crypto isakmp key cisco address 172.19.152.48 <= Unreachable peer
crypto isakmp key cisco address 192.168.1.104
!
crypto map mymap 1 ipsec-isakmp
  set peer 172.19.152.48 <= Unreachable peer
  set peer 192.168.1.104
  set security-association lifetime seconds 120
  set transform-set TSET3
  match address 101
!
```

- 3) Once the tunnel is up, ping 880 from the peer continuously.
- 4) Do a “clear crypto session” on 880.
- 5) Try to ping the peer from 880.
- 6) Tracebacks will appear and sometimes the system crashes.

- CSCto39885

Symptoms: A router crashes.

Conditions: gcid and callmon is turned on.

Workaround: There is no workaround.

- CSCto48060

Symptoms: A Cisco 3900 series router may crash with the following error:

```
Unexpected exception to CPU: vector 1400
```

Conditions: The symptom is observed when the router is configured as a voice gateway using H323 and H245 and connected to CUCM. If CUCM is sending a MultiMediaSystemControl messages with no entry, the router may crash.

Workaround: There is no workaround.

- CSCto55643

Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

Workaround: There is no workaround.

- CSCto60047

Symptoms: A crash occurs either due to a chunk corruption or at `ssh_send_queue_data`.

Conditions: This symptom occurs under the following conditions:

- An SSH session exists between two routers.
- The **show tech** command is issued and then aborted.

Workaround: There is no workaround.

- CSCto63268

Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

Workaround: Remove the EVM or disable DSP sharing.

- CSCto72480

Symptoms: The output of the **show mfib linecard** command shows that line cards are in “sync fail” state.

Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

Workaround: If this issue is seen, using the **clear mfib linecard slot** command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto72927

Symptoms: Configuring an event manager policy may cause a cat4k to hang.

Conditions: Configuring a TCL policy and copying that policy to the device.

Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.7/3.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C>

No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCto73345

Symptoms: A router crashes while reloading after configuring a crypto IPsec manual keying policy.

Conditions: This issue is seen when a router that is configured with a crypto IPsec manual keying policy is reloaded.

Workaround: There is no workaround.

- CSCto86833

Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DN's with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

Workaround: If possible, reduce the number of voice ports automatically generated by the number DN's and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- CSCto88393

Symptoms: CPU hogs are observed on a master controller:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0),process = OER Master Controller.
```

Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

Workaround: There is no workaround.

- CSCto89536

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw>

- CSCtq12007

Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less severe; you may see one every other packet drop, until the next rekey or tunnel reset.

Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq21234
Symptoms: Label is not freed.
Conditions: The symptom is observed after shutting down the link.
Workaround: There is no workaround.
- CSCtq24733
Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.
Conditions: The symptom is observed with MRCP is enabled.
Workaround: There is no workaround.
- CSCtq25682
Symptoms: The router crashes after configuring “gw-accounting file”.
Conditions: This symptom occurs if the router’s memory usage is already over 80 percent utilization, and after configuring “gw-accounting file”, the following log message is displayed:

```
%VOICE_FILE_ACCT-4-MEM_USAGE_HI_WATERMARK: System memory on high usage (81/100).  
Stopping processing new event log for now.
```


After this log, when the cdrflush-timer expires, the router crashes.
Workaround: Do not enable “gw-accounting file” when the router’s memory utilization is already over 80 percent.
- CSCtq26892
Symptoms: CUBE crashes @ sipSPI_ipip_IsHdrInHeaderList.
Conditions: This symptom is observed with a PRACK-NO PRACK configuration on Cisco IOS Release 15.2(1)T.
Workaround: There is no workaround.
- CSCtq32896
Symptoms: LSM entries stop forwarding traffic.
Conditions: This symptom is observed after Stateful Switchover (SSO).
Workaround: There is no workaround.
- CSCtq36153
Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:
 - Memory Leak Associated with Crafted IP Packets
 - Memory Leak in HTTP Inspection
 - Memory Leak in H.323 Inspection
 - Memory Leak in SIP Inspection
 Workarounds that mitigate these vulnerabilities are not available.
Cisco has released free software updates that address these vulnerabilities.
This advisory is available at the following link:
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfbw>

- CSCtq45553

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfbw>

- CSCtq47428

Symptoms: A Cisco router acting as an SRST may unexpectedly reload due to a bus error.

Conditions: This symptom is observed with phones registered to the SRST.

Workaround: There is no workaround.

- CSCtq49325

Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq55173

Symptoms: A device that is configured with NAT crashes. SIP appears to be translated through NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

Workaround: There is no workaround.

- CSCtq56727

Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash.

The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP, and other processes.

“sh proc mem sorted” shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

Conditions: This symptom occurs when the SIP trunk in Unified Communications Manager pointing to the gateway is configured with a DTMF signaling type of “no preference” and the SIP gateway is configured with DTMF relay as sip-kpml.

Workaround: There are two workarounds:

1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”

Recovery: In order to recover from the crash, you must reload the gateway router.

- CSCtq58383

Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq61128

Symptoms: Router is crashing with Segmentation fault(11)

Conditions: It was observed on routers acting as IPSEC hub using certificates.

Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2011-4231 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq75008

Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

Conditions:

- The Cisco 7206 VXR works as a server for L2TP over IPsec.
- Encryption is done using C7200-VSA.
- More than two clients are connected.

If client sessions are kept up for about a day, the router crashes.

Workaround: There is no workaround.

- CSCtq80648

Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

For example:

```
interface Ethernet1/0
  vrf forwarding vpn1
  ipv6 address 1::1/64
!
router bgp 65000
  address-family ipv6 vrf vpn1
    neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq83629

Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

Workaround: Line card reload is required to resolve the problem.

- CSCtq85728

Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.

Workaround: There is no workaround.

- CSCtq88777

Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq92940

Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtq97991

Symptoms: ADSL interface fails to re-train when “dsl enable-training-log” is configured.

Conditions:

1. Observed in a Cisco 800, 1900, and 2900 chassis and could affect other software platforms.
2. Observed in Cisco IOS Release 15.1(2)T, Release 15.1(2)T1, and Release 15.1 (3)T. 3. It is not observed in Cisco IOS Release 15.0(1)M4.

Deviation observed in the following manner:

1. With “dsl enable-training log” not configured the HWIC trains up to the DSLAM OK. After unplugging cable and reconnecting it, the HWIC still comes up fine after.
2. Configure “dsl enable-training log”. After unplugging cable and reconnecting it, the HWIC fails to come up. CD LED does not blink and the following error message appears: “No retrain. sleep 20 seconds”.

Workaround: Remove “dsl enable-training-log.”

- CSCtr04829

Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

Conditions: This symptom occurs when the hardware address is zero.

Workaround: There is no workaround.

- CSCtr06747

Symptoms: ISIS neighborship remains in INIT state when MTU at both ends is changed to 4470.

Conditions: The symptom is observed when a Cisco 2900 is used in the topology with MTU 4470 (any MTU > 2000).

Workaround: Replace the Cisco 2900 with a Cisco 2800 or reduce the MTU to < 2000.

- CSCtr11620

Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

Conditions: This symptom is observed when a Cisco 2911 is used.

Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr15891

Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

Workaround: There is no workaround.

- CSCtr18574

Symptoms: H323-H323 video calls fail with cause code 47.

Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:

Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
 cch323_send_passthru_out: Send passthru message retcode 15

Workaround: There is no workaround.

- CSCtr25821

Symptoms: A Cisco 800 series router crashes with **isdn leased-line bri0 128** command:

Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310

Conditions: The symptom is observed with the **isdn leased-line bri0 128** command.

Workaround: The issue does not occur if there is no cable that connects to the BRI interface. Disconnect the cable from the BRI interface while the **isdn leased-line bri0 128** command is configured.

- CSCtr28857

A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

- CSCtr29338

Symptoms: A router crashes.

Conditions: The symptom is observed after a “%ISDN-6-DISCONNECT” message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

Workaround: There is no workaround.

- CSCtr44686

Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
  class type inspect smtp SMTP_L7_C1
    reset
policy-map type inspect smtp SMTP_L7_P2
  class type inspect smtp SMTP_L7_C2A
    reset
  class type inspect smtp SMTP_L7_C2B
    reset
```

Conditions: The symptom is observed with the above maps.

Workaround: Replace “reset” with “log”.

- CSCtr45608

Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr46123

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

- CSCtr49064

The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh>

- CSCtr51926

Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

Conditions: The symptom is observed when a service-policy is applied on the main interface.

Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y
  ipv6 enable
```

Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z
  no ipv6 address
  ipv6 address ...
```

- CSCtr54269

Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr54327

Symptoms: A Cisco router may crash due to a SegV exception or have a spurious access when a fax comes in.

Conditions: The crash occurs on a voice gateway that is configured with transcoding and fax passthrough where a fax call comes in for a codec, but the fax is not configured for a codec, and the “a=silenceSupp:off” option is set in SDP.

Workaround: There is no workaround.

- CSCtr58140

Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

Workaround: There is no workaround.

- CSCtr79347

Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
Traceback summary % 0x80e7b6 : __be_bgp_tx_walker_process % 0x80e3bc :
__be_bgp_tx_generate_updates_task % 0x7f8891 : __be_bgp_task_scheduler
```

Conditions: No conditions but this is a rarely observed issue.

Workaround: There is no workaround.

- CSCtr86437

Symptoms: NAT-PT function does not work properly after an interface flap occurs.

Conditions: The symptom is observed when you configure NAT-PT on the router.

Workaround: Reconfigure “ipv6 nat prefix.”

- CSCtr91106

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

- CSCtr92779

Symptoms: Call scenario is with Avaya CM6 over TLS/SIP trunks, which causes the Cisco 3945 router (running Cisco IOS Release 15.1(4)M1) CUBE to crash.

Conditions: The symptom is observed when a call is originated from Cisco Phone A via TLS/SIP Trunk to CUBE (3945 15.1(4)M1) to Avaya CM6 Phone A, which is set to “call forward all” back to the original Cisco Phone A.

Workaround: There is no workaround.

- CSCtr97640

Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

Conditions: None.

Workaround: None. Physically securing the router is important.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.9/1.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C>

CVE ID CVE-2011-3289 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts06929

Symptoms: Disposition traffic gets dropped after SSO as the new local labels allocated by AToM do not get programmed on the line cards.

Conditions: This symptom occurs when pseudowires are configured on the setup without graceful restart configured. Then, SSO is performed and two local labels have the same disposition information. This really manifests as a traffic drop issue when the scale is high.

Workaround: Configuring graceful restart resolves this issue.

- CSCts16285

Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts28315

Symptoms: A DHCP PD request does not accept a specific server.

Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

<http://tools.ietf.org/html/rfc3633#section-10>

A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

Workaround: There is no workaround.

- CSCts33952

Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

Workaround: There is no workaround.

- CSCts38429

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike>

- CSCts39535

Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts40771

Symptoms: Device goes into a hang state and requires a power cycle. If “scheduler isr-watchdog” is configured, the device will crash and reload the system.

Conditions: This issue has been seen with “ip nbar protocol-discovery” configured on tunnel interfaces.

Workaround: Remove “ip nbar protocol-discovery” from the device.

- CSCts59014

Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

Workaround: There is no workaround.

- CSCts64539

Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts76410

Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts78348

Symptoms: Packet drop will occur on a router when the interface is configured as 10/full.

Conditions: It seems that when interface is configured as 10/full, with the traffic of 10 Mbps, this issue will occur. By performing a shut/no shut on the interface, this issue will recover but it will be seen again when you reload the device.

This issue may be seen on a Cisco 19xx and a Cisco 29xx (except Cisco 2951) This issue may occur when manual set duplex on the affected platform.

Workaround 1: Perform a shut/no shut on the interface and this issue will recover.

Workaround 2: Use auto negotiation.

- CSCts80643

Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

A workaround is available to mitigate this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp>

- CSCtt11210

Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt16051

Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall>

- CSCtt17879
Symptoms: The **bgp network backdoor** command does not have any effect.
Conditions: This symptom occurs:
 - On 64-bit platform systems.
 - When the network is learned after the backdoor has been configured.
 Workaround: Unconfigure and reconfigure the network backdoor.
- CSCtt20215
Symptoms: Controller goes down after reload.
Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.
Workaround: Unplug/plug the cable, or reset link from PBX side.
- CSCtt96597
Symptoms: Unable to power-cycle modem using **test cellular unit modem-power-cycle**.
Conditions: The symptom is observed when a router cannot communicate with the modem due to a possible modem firmware crash or device disconnect.
Workaround: Reload router.
- CSCtt98801
Symptoms: Mobile router reports stale RRP received from HA.
Conditions: The symptom is observed when the mobile router sends a RRQ to HA in CCOA mode.
Workaround: There is no workaround.
- CSCtu07626
Symptoms: Router processing SIP traffic crashes.
Conditions: The following error may be seen prior to the crash:

```
%SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to process.
```

 Workaround: There is no workaround.
- CSCtw67599
Symptoms: IPsec tunnels do not come up.
Conditions: This symptom is observed in Cisco IOS Release 15.1(3)T2.3, which uses a hardware crypto engine.
Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)T2

Cisco IOS Release 15.1(3)T2 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T2 but may be open in previous Cisco IOS releases.

- CSCso33003
Symptoms: If a child policy is attached to a parent policy twice, the router will reload if the child policy configuration is removed.
Conditions: The parent policy needs to be attached to the target interface.

Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCtb24959

Symptoms: The router may crash while clearing a large number of RP mappings.

Conditions: This symptom occurs when you configure the router as an RP agent and candidate RP for a large number of RPs. This issue is seen when you run the **clear ip pim rp-map** command several times.

Workaround: Do not run the **clear ip pim rp-map** command several times in succession.

- CSCtb74547

Symptoms: A Cisco ASR 1000 DMVPN HUB reloads at the process IPsec key engine.

Conditions: This symptom is observed when the “Dual DMVPN with Shared Tunnel-Protection” feature is enabled and the interface is shut down and brought up again.

Workaround: There is no workaround.

- CSCtd23069

Symptoms: A crash occurs because of a SegV exception after configuring the **ip virtual-reassembly** command.

Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd90030

Symptoms: A Cisco 2851 router may crash with a bus error.

Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. This issue is seen with Cisco IOS Release 12.4(24)T1 or Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtf39056

Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.

Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be to set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
#####
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
#####
```

- CSCtg54878

Symptoms: Static routes with only the name option are not installed in the route table.

```

Router(config)#ip route <des ip add> <sub mask> <ip add> name test track
101
                                ^^^^^^
                                name option

Router#sh runn | sec track
      ip route <des ip add> <sub mask> <ip add> name test track 101

Router#show ip route track
      ==> ip route <des ip add> <sub mask> <ip add> name test track 101 is
not installed

```

Conditions: This symptom is observed with static routes that have only the name option.

Workaround: Instead of using `ip route <des ip add> <sub mask> <ip add> name test track`, use the following:

```
ip route <des ip add> <sub mask> <ip add> intf track name test
```

For example:

```
ip route 1.1.1.1 255.255.255.255 e0/0 track 1 name abc
```

- CSCtg72652

Symptoms: On Cisco 2900 series routers, the following warning message might display on the console:

```
%ENVMON-1-POWER_WARNING: : Chassis power is not good in the PSU 1
```

Conditions: Under rare conditions, the power supply sometimes sends a false alarm status to the system, even though the system power is working fine.

Workaround: There is no workaround.

- CSCtg84969

Symptoms: The output of **show ip mfib vrf vrf-name verbose** may show the following line “Platform Flags: NP RETRY RECOVERY HW_ERR” and multicast traffic may not be hardware switched.

Conditions: The symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSOs. When the issue occurs, the output of **show ip mfib vrf vrf-name verbose** on the standby SP will show some lines preceeded with “###” where an interface name is expected.

Workaround: There is no workaround.

- CSCtg89555

Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

Conditions: This symptom is observed when configuring an IP address after multicast has been configured on a dot1Q interface.

Workaround: Performing a shut/no shut of the interface will fix the problem.

- CSCth01526

Symptoms: The MDT interface is deactivated and activated after an SSO.

Conditions: This symptom is observed after an SSO, when the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

Workaround: There is no workaround.

- CSCth11006

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCth85294

Symptoms: A PIM neighborship is not established with the remote PE and RP for the MVRFs.

Conditions: This symptom is observed with traffic and after removal and restoration of MVRFs. Traffic does not flow properly as the PIM neighborship is not established with the remote PE and RP for those MVRFs.

Workaround: There is no workaround; however, multiple removals of MDTs could help.

- CSCth87458

Symptoms: Memory leak is detected in `ssh_buffer_get_string`.

Conditions: Use test tool Codenomicon to test SSH verification against UUT (SSH-Server test). After the test, the memory leak will be seen in `ssh_buffer_get_string`.

Workaround: There is no workaround.

- CSCti18615

Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP being out of sync with the active RP. The A and F flags are missing from the multicast forwarding base entries.

Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, and when the router is in HA mode SSO and is reloaded from the RP.

Workaround: Perform a shut/no shut of the affected interfaces.

- CSCti25459

Symptoms: The device might crash with `fib_forw_add_extra_encap_and_forward`. Also, possibly ICMP packets with unreachable sourced may be seen.

Conditions: This symptom is observed when MLPS is enabled on these devices.

Workaround: Use NAT NVI instead of legacy NAT.

- CSCti40660

Symptoms: The following message is displayed:

```
%FW-4-GLOBAL_SESSIONS_MAXIMUM: Number of sessions for the firewall exceeds the
configured global sessions maximum value 2147483647
```

Conditions: This symptom is observed when IP SLA is configured along with self zones.

Workaround: There is no workaround.

- CSCti48504

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>.

- CSCtj04672

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCtj05903

Symptoms: Some virtual access interfaces are not created for VT, on reload.

Conditions: This symptom occurs on scaled sessions.

Workaround: There is no workaround.

- CSCtj15090

Symptoms: The IPv6 connection setup between Cisco IOS Release 12.4 and Cisco IOS Release 12.2 fails.

Conditions: This symptom occurs when the Sender (or responder) is running Cisco IOS Release 12.4 and the Responder (or sender) is running Cisco IOS Release 12.2. Because of a message mismatch, the control message for IPv6 fails.

Workaround: Use “control disabled”, as there is no workaround if control is enabled.

- CSCtj23189

Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.

Conditions: This symptom occurs only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with three classes: one with 16 kbps, the second one with 1 Mbps, and the third one with 99 Mbps.

Workaround: There is no workaround.

- CSCtj33003

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip>

- CSCtj36521

Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

Workaround: Ensure that IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj84234

Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

```
route-map <RM name>
  match ip address <acl>
  set ip next-hop <NH1> <NH2>
```

Workaround: There is no workaround.

- CSCtj87846

Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is a backup.

Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtk02814

Symptoms: The **show pppoe throttled subinterfaces** command output is truncated, and does not show throttled ATM VC or QinQ subinterfaces during throttling.

Conditions: This symptom occurs when PPPoE throttling is configured and active.

Workaround: There is no workaround.

- CSCtk12681

Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk18607
Symptoms: The router crashes at `ssh_pubkey_command_nvgen` and `ssh_pubkey_nvgen`.
Conditions: This symptom occurs at `ssh_pubkey_command_nvgen` and `ssh_pubkey_nvgen`.
Workaround: There is no workaround.
- CSCtk31401
Symptoms: A Cisco router crashes when the SSH session from it is exited.
Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.
Workaround: There is no workaround.
- CSCtk36891
Symptoms: Video conferencing through NAT may crash the router.
Conditions: This symptom occurs when NAT is configured to perform ALG processing on SKINNY messages. As a result, video conferencing with PVDm3 crashes the router.
Workaround: Disable NAT ALG processing of SKINNY messages using the **no ip nat service tcp port** command, where *port* is the port number used by the SKINNY protocol. The default SKINNY port is 2000. So, if SKINNY is using the default port, then the command would be “no ip nat service tcp port 2000”.
- CSCtk52807
Symptoms: Processor pool memory corruption crash is observed.
Conditions: This condition occurs when VoIP/SIP is enabled.
Workaround: Upgrade the phone load to SCCP42.9-1-1SR1S or later and decrease hunt group timeouts.
- CSCtk62950
Symptoms: SSH over IPv6 may crash the router.
Conditions: This symptom occurs with SSH over IPv6.
Workaround: There is no workaround.
- CSCtk67073
The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.
Cisco has released free software updates that address this vulnerability.
This advisory is posted at
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla>.
- CSCtk68647
Symptoms: The Cisco ASR is configured as a DMVPN hub and spoke connections fail to rekey or initially connect after the box has been up for some time. The length of time is based on the number of connections. In addition, the **show crypto sockets** command output shows that sockets are leaking and do not release even when the SA is inactive.
Conditions: This symptom is observed with the Cisco ASR code prior to Cisco IOS XE Release 3.2.0. This issue is seen with multiple DMVPN tunnels configured with tunnel protection and the **shared** keyword.

Workaround: Upgrade the Cisco ASR code to Cisco IOS XE Release 3.2.0. Remove other DMVPN tunnels (or shut them down).

- CSCtk74660

Symptoms: The Network Time Protocol (NTP) tries to resync after the server clock changes its time and after the NTP falls back to the local clock.

Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

Workaround: There is no workaround.

- CSCtk98021

Symptoms: Portions of the WebVPN/SSL VPN code in the Cisco IOS needs to be enhanced to address secure coding best practices.

Conditions: This symptom occurs with a Cisco IOS device configured for WebVPN/SSL VPN.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.9:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:POC/RL:U/RC:C>

No CVE ID has been assigned to this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtl00467

Symptoms: A Cisco router crashes.

Conditions: This symptom is observed when call monitoring is enabled and the "conference call" feature is used.

Workaround: There is no workaround.

- CSCtl05684

Symptoms: Xauth user information remains in the **show crypto session summary** command output.

Conditions: This symptom is observed when running EzVPN and if Xauth is performed by a different username during P1 rekey. This issue is seen when NAT is used in the VPN path.

Workaround: Use the save-password feature (without interactive Xauth mode) to avoid sending a different username and password during P1 rekey.

- CSCtl20509

Symptoms: In CME/SRST 4.0, when ATA unregister/fall back to the Cisco Unified CallManager, the virtual POTS dial peers stay up and calls to ATA do not go out the H323 dial peer to the Cisco Unified CallManager. The calls fail with user busy. This issue affects only ATA. Dial peers of the IP phones behave normally.

Conditions: This symptom occurs when the ATA fallback to the CCM occurs and registers with the CCM. However, the virtual POTS dial peers for the ATA are up.

Workaround: Reload the router.

- CSCtl43156

Symptoms: When using a BVI interface configured for IPv6 on a Cisco ISR-G2 series router, IPv6 neighbors are never discovered over the BVI. Neighbors will never be seen in the **show ipv6 neighbors** command output and all traffic to/through the BVI will fail.

Conditions: This symptom occurs when IPv6 is configured on Cisco ISR-G2 router images running on the “datak9” package.

Workaround: Use the “uck9” technology package, where the IPv6 feature is already present.

- CSCtl45684

Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

```
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
```

Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.

Workaround: There is no workaround.

- CSCtl53899

Symptoms: SIP to SIP calls through CUBE may cause memory corruption when resource priority passthrough is enabled on the dial peers.

Conditions: This symptom is observed on CUBE with Cisco IOS Release 15.1(3)T, where the following was configured under the SIP dial peers:

```
voice-class sip resource priority mode passthrough
```

Workaround: Disable memory lite allocations using the **no memory lite** command. This will increase the size of memory allocations, so be careful when using it on a device with high memory utilization.

- CSCtl67079

Symptoms: The following error message is seen on a Cisco router with HWIC_1GE_SFP inserted:

```
%HWIC_1GE_SFP-3-INTERNAL_ERROR: GigabitEthernet0/0/0 SNMP high capacity
counter register failed
```

Conditions: This symptom is observed during bootup.

Workaround: There is no workaround.

- CSCtl94813

Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analog phone on the VG224 attends a conference bridge. It causes one-way audio.

- When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen.
- For the same call, the PCM trace shows no audio in the RIN stream.

Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

```
*Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx:
Got RX stats
Packet details:
  Packet Length=188, Channel Id=1, Packet Id=200
  RX Packets=0: Signaling=0, ComfortNoise=0
  Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms)
  Packet Counts: OOSquence=0, Bad header=0, Late=0, Early=0Receive
inactive duration=129(ms)
```

Workaround: Downgrade the Cisco IOS to Cisco IOS Release 12.4(4)T8.

- CSCtl95752
Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.
Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.
Workaround: There is no workaround.
- CSCtl98132
Symptoms: XDR CPU hog may cause system crash.
Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.
Workaround: There is no workaround.
Further Problem Description: The crash can be avoided if the system has no double failure.
- CSCtn04686
Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unplugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.
Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.
Workaround: Unplug/plug the cables.
- CSCtn08208
Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.
Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.
Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.
- CSCtn08258
Symptoms: The router crashes.
Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T2 and Cisco IOS Release 15.1(3)T1 when SIP calls are made.
Workaround: There is no workaround. However, this issue is not seen in Cisco IOS Release 15.1(4)M.
- CSCtn10922
Symptoms: A router configured with “atm route-brridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.
Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-brridged ip” and forwarding multicast traffic.
Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.
- CSCtn12119
Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.
Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such, no workaround is necessary from a usability perspective. The image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn19178

Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf “A” and a new local label will not be reassigned.

Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf “B”, including:

- The vrf interface, for example, **no interface Gi1/0/1.430**.
- The same vrf process, for example, **no router ospf process id vrf vrf name**.

Run the following commands to verify whether you are facing this issue:

- **show ip bgp vpnv4 vrf A subnet** (this is for the working vrf)
- **show mpls forwarding-table labels local label**

Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

- **clear ip bgp mp-bgp neighbor soft in**
- **clear ip bgp mp-bgp neighbor soft out**

- CSCtn19496

Symptoms: Packet loss is seen when the service policy is applied on the tunnel interface. The **show hqf interface** command output shows drops in a particular queue with the following:

```
Scheduler_flags 177
```

The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.

Conditions: This symptom is observed when the service policy is applied on the tunnel/GRE interface, and when the source of the tunnel interface is the ATM interface (hwic-shdsl).

Workaround: There is no workaround.

Further Problem Description: The above-described symptom is seen only with the SHDSL link.

- CSCtn26785

Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

```
3845#sh int atm 1/0 stat
ATM1/0
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
Processor         98170      10995040    1           68
Route cache       0          0           98170       10995040
Total             98170      10995040    98171       10995108
3845#
```

```
3845#sh cef int atm 1/0
ATM1/0 is up (if_number 5)
  Corresponding hwidb fast_if_number 5
  Corresponding hwidb firstsw->if_number 5
  Internet address is 64.65.248.174/30
  ICMP redirects are never sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Input features: Ingress-NetFlow
  Output features: Post-Ingress-NetFlow
```

```

IP policy routing is disabled
BGP based policy accounting on input is disabled
BGP based policy accounting on output is disabled
Hardware idb is ATM1/0
Fast switching type 9, interface type 138
IP CEF switching enabled
IP CEF switching turbo vector
IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
Input fast flags 0x0, Output fast flags 0x0
ifindex 5(5)
Slot Slot unit 0 VC -1
IP MTU 4470
3845#

```

Conditions: The conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn38996

Symptoms: All MVPN traffic is getting blackholed when a peer is reachable using a TE tunnel, and an interface flap is done so that the secondary path can be selected. The multicast route does not contain a native path using the physical interface.

Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn48744

Symptoms: Memory leaks on OER border router while running the PfR-IPSLA configuration.

Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

Workaround: There is no workaround.

- CSCtn53094

Symptoms: The router crashes or generates the following error:

```
%SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process=
"Mwheel Process", ipl= 2, pid= 315
```

Conditions: This symptom is observed when toggling very fast between the **ip pim mode** and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

Workaround: Avoid fast toggling of the **pim mode** command if possible when it is only present on a single interface.

- CSCtn58128

Symptoms: The BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

Conditions: This symptom may be triggered by route-flaps in scaled scenario, where the route reflector may have 4000 route reflector clients and processing one million+ routes.

Workaround: Ensure that “no logging console” is configured.

- CSCtn65060

Symptoms: A Cisco device crashes.

Conditions: This symptom is observed with Cisco IOS Release 15.0M and Cisco IOS Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”

Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.

- CSCtn69929

Symptoms: The DHCP server does not assign any addresses to clients, even though smart-install is configured with DHCP pool parameters.

Conditions: This symptom occurs when smart-install is configured to assign DHCP addresses.

Workaround: Execute the **show running-configuration** command on the box once.

- CSCtn72939

Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.

Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.

Workaround: Configure bridge-group under that xconnect interface.

- CSCtn76183

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

- CSCtn87012

Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

Workaround: Pick up the phone during the ringing OFF cycle.

- CSCtn91807

Symptoms: A router acting as a voice gateway may crash due to a bus error.

Conditions: This symptom occurs when a button is pressed on a phone while using skinny. However, the exact conditions that cause this symptom are currently unknown.

Workaround: There is no workaround.

- CSCtn93891

Symptoms: Multicast traffic is getting blocked.

Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

Workaround: There is no workaround.

- CSCtn96521

Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast peer** command on the router.

Conditions: This symptom occurs with the following conditions:

Router3 ---ebgp--- Router1 ---ibgp--- Router2

```
ROUTER1:
-----
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
!

router ospf 100
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.3 remote-as 11
!

ROUTER2:
-----
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 100
 redistribute static
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

ROUTER3:
-----
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip pim sparse-mode
!
router bgp 11
 bgp log-neighbor-changes
 network 0.0.0.0
 network 0.0.0.0 mask 255.255.255.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.

2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCto00318

Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

For now, consider not initiating a SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

Workaround: There is no workaround.

- CSCto00796

Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

Conditions: This symptom occurs when a new interface is provisioned inside a VRF and the configuration such that the connected routes are redistributed in the VRF. This redistributed route fails to tag itself with the RT when it reaches the peering PE (+RR)

Workaround: Soft clear the peer that missed getting the RT.

- CSCto02448

Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

Conditions: This symptom is observed with the following conditions:

1. The neighbor is configured with soft-reconfiguration inbound.
2. The inbound routemap is not configured for the neighbor.
3. The non-routemap inbound policy (filter-list) allows the path.

Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto03446

Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

Conditions: This symptom occurs with a flat policy attached to frame-relay interface with traffic shaping enabled.

Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto07586

Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

Conditions: This symptom occurs with the following conditions:

1. Create an IOS image that does not IPV6 enabled.
2. Enable BFD on an interface.
3. Configure an IPV4 static route with BFD routing through the above interface.

The IPV4 BFD session does not get established, so the static route does not get installed.

Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

- Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
- ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>

- CSCto08754

Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.

Conditions: This symptom occurs when the crypto VTI interface becomes wedged.

Workaround: There is no workaround.

- CSCto11025

Symptoms: When traffic streams are classified into multiple classes included with LLQ on the tunnel interface and the crypto map applied to an interface, packets are dropped on crypto engine with buffers unavailable.

Conditions: This symptom occurs when configuring GRE over IPSec with a crypto map on the main interface. This issue is seen when the QoS policy is configured, and there is congestion.

Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- CSCto13254

Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

```
Hash verification failed for file <temp location of profile>
```

Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

Workaround: Remove the profile from the Cisco IOS headend.

- CSCto13338

Symptoms: When a PSTN phone is calling an IP phone that is forwarded to a PSTN destination, the call is placed but no audio is present. This is the same behavior with blind transfer to external destinations.

Conditions: This symptom occurs when voice-class codec X offer all and transcoders are used with CUBE.

Workaround 1: Use the **codec XXXX** command instead of voice-class codec X offer all.

Workaround 2: Use consultative transfer instead of blind transfer.

- CSCto15361

Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

Conditions: This symptom occurs when the Active Supervisor crashes while disabling the IPv6 router EIGRP because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

Workaround: Modify the `igrp2_procinfo_free` function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16597

Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.

Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.

Workaround: There is no workaround.

- CSCto23807

Symptoms: A Cisco device crashes when trying to transfer a call.

Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T2.

Workaround: There is no workaround.

- CSCto24338

Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0XXXXXXXXX
```

Conditions: This symptom occurs with NAT+SIP.

Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

- CSCto31265

Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

Workaround 1: Delete/readd the static route that generates Type7.

Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto34844

Symptoms: The Cisco 891 may perform lower than the older generation Cisco 1812 platform.

Conditions: This symptom occurs when Ethernet traffic using the VLAN tag is encapsulated inside the L2TPv3 tunnel.

Workaround: There is no workaround.

- CSCto41165

Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit/deny** command, and then the **no ip extcommunity-list 55 permit/deny** command.

Conditions: This symptom occurs when the standby router is configured.

Workaround: There is no workaround.

- CSCto41173

Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.

Conditions: This symptom is observed with a platform that acts as an H323 gateway and runs Cisco IOS Release 15.1(3)T.

Workaround: Revert to Cisco IOS Release 12.4(20)T.

- CSCto44581

Symptoms: The router crashes on high call volume.

Conditions: This symptom occurs on high call volume.

Workaround: There is no workaround.

- CSCto46716

Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto47524

Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs Responder.

A **show process memory sorted** command may initially show “MallocLite” growing. By disabling mallocite with the following:

```
config t
no memory lite
end
```

One may start to see the process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80MB per day.

Conditions: This symptom is observed on a Cisco ASR 1002 router.

Workaround: Disable IP SLA on the affected router, if possible.

- CSCto50255

Symptoms: Memory leak occurs while running the UDP echo operation.

Conditions: This symptom is observed when a UDP echo operation successfully runs. The leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory pid** command.

Workaround: There is no workaround.

- CSCto53332

Symptoms: A router configured for IPSec accounting may display the following error message:

```
%AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
```

This does not seem to result in any impact apart from intermittently lost accounting messages.

Conditions: This symptom occurs when IPSec accounting is active.

Workaround: There is no workaround.

- CSCto63417

Symptoms: A spurious access or crash occurs after applying the service policy.

Conditions: This symptom occurs specifically when applying service-policy type access-control. This issue occurs when a large amount of traffic is being sent to the interface. The class-map uses RegEx in the match statement.

For example:

```
class-map type access-control match-any bittorrent
  match start l2-start offset 54 size 32 regex "GETinfo_hash="
  match start l2-start offset 54 size 32 regex
"[a|A][z|Z][v|V][e|E][r|R]
```

Workaround: Apply the service policy during low traffic or do not use RegEx in match statements.

- CSCto63954

Symptoms: A router with GETVPN configurations is continuously crashing.

Conditions: This symptom is seen with GETVPN related configurations with the fail-close feature activated.

Workaround: There is no workaround.

- CSCto68554

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>.

- CSCto71744

Symptoms: FXO interfaces with the cable-detect feature enabled will automatically transition to the off-hook state when no PSTN battery voltage is detected, and remain off-hook for a duration of up to 1 minute. This condition violates regulatory telecom standards in several countries, including but not limited to the USA and Canada.

The failing clauses of regulatory standards are as follows:

- TIA-968-B 5.1.11.3
- TIA-968-B 5.1.12.3
- Industry Canada CS-03 Part I, Issue 9 December 2010

Conditions: This symptom occurs when the FXO interface is up, and the cable is connected to PSTN. Any interruption of the PSTN battery to FXO induces the off-hook condition, and the port does not transition back to on-hook for up to 1 minute.

Workaround: Disable the cable-detect feature in the FXO <config-voiceport> prompt. You can enable the feature in topologies that are not subject to regulatory standards (that is, on-premise installations).

- CSCto81814

Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

Conditions: This symptom is observed only when ECDSA certificates are used for IKEv2 and not with RSA certificates or with IKEv1.

Workaround: There is no workaround.

- CSCto88686

Symptoms: UCM cores when receiving SIPPublishReq with port “0”.

SDI trace:

```
13:15:18.735 |//SIP/Stack/Transport/0xd1e9460/msg=0xb7cee278, addr=xxx.xxx.xxx.xxx,
port=0
```

Conditions: This symptom occurs with the following conditions:

- Configure the SIP trunk destination address as an IP address. The destination address is an SRV checkbox that is not checked.
- Destination port = 0.

Workaround: Modify the SIP trunk configuration to utilize a port in the defined valid port range between 1024 and 65535.

- CSCto99523

Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

Conditions: This symptom occurs when convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

Workaround: There is no workaround.

- CSCtq04117

Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loopback. OSPF provides reachability to BGP next hop, and BFD is running.

Conditions: This symptom occurs under the following conditions:

1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

Workaround: Use the **clear ip route vrf x *** command.

- CSCtq05004

Symptoms: Dialer loses the IP address sporadically. Shut/no shut on the ATM interface does not help.

Conditions: There are no conditions so far. The behaviour is sporadic.

Workaround: Reload.

- CSCtq05636

Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg.

For example:

```
Received:
INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0

Sent:
INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
```

In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq06538

Symptoms: The RP crashes due to bad chunk in MallocLite.

Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

```
LOCAL_PREF
Header
  AttributeFlags
    Optional: 0b0
    Transitive: 0b1
    Partial: 0b0
    ExtendedLength: 0b0
    Unused: 0b0 0b0 0b0 0b0
  TypeCode: 0x05
  Length: 0x01      <----- should be 0x04 instead
  Value: 0xff 0xff 0xff 0xff
  NetworkLayerReachabilityInfo: 0x08 0x0a <snip>
```

Workaround: There is no workaround.

- CSCtq09899

Symptoms: The VXML gateway crashes.

Conditions: This symptom occurs during the load test, when the **show mrcp client session active** is used.

Workaround: There is no workaround.

- CSCtq10684

Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in IPSec.

Conditions: This symptom occurs when tunnel flap is observed before the crash.

Workaround: A possible workaround is to reload the box.

- CSCtq15247

Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

For example:

```
LAC1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
LAC1(config)#interface virtual-ppp1
LAC1(config-if)#no pseudowire
LAC1(config-if)#exit
LAC1(config)#no interface virtual-ppp1
```

- CSCtq27180

Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.

Conditions: This symptom is observed only on IOS internal releases.

Workaround: There is no workaround.

Further Problem Description: The following LOG messages and errors are found:

```
Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed
-Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z
63765DE4z 63765DC8z
Mar 30 01:27:38.447: %LICENSE-2-VLS_ERROR: 'VLSsetInstallLicenseStorage'
failed with an error - rc = 136 - 'Error[136]: Specified license store
doesn't exists.'
-Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z
63765DC8z
```

- CSCtq28151

Symptoms: A bus error crash occurs.

Conditions: This symptom is observed on a Cisco 3900 voice gateway running Cisco IOS Release 15.1(3)T1.

Workaround: There is no workaround.

- CSCtq28732

Symptoms: Memory leak is observed when device is configured **parameter-map type inspectglobal**.

Conditions: Device is configured with **parameter-map type inspect global**.

See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfb>

Workaround: There is no workaround.

- CSCtq29554

Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

Workaround: Reload the failing line card to recover it.

- CSCtq30875

Symptoms: A Cisco ISR G1 will display “March 11, 2011” when the **show clock** command is entered. This will effect functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

Workaround: The clock can be set manually via CLI.

- CSCtq39406

Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

Conditions: This symptom occurs when you set up an energywise domain via the CLI, and then set the energywise level to zero on a SM or ISM.

Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- CSCtq49408

Symptoms: Analog phone calls (fxs) cannot be made with CME/SCCP.

Conditions: This symptom occurs when SCCP support for FXS is missing in IAD2435.

Workaround: There is no workaround.

- CSCtq61850

Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

Workaround: There is no workaround.

- CSCtq62322

Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).

Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.

Workaround: There is no workaround.

- CSCtq62759

Symptoms: The CLNS routing table is not updated when the LAN interface with CLNS router ISIS configured shuts down because ISIS LSP is not regenerated. The CLNS route will be cleared after 10 minutes when ISIS ages out the stale routes.

Conditions: This symptom is seen when only the CLNS router ISIS is enabled on the LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq64951

Symptoms: The following message is displayed:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto
functionality with securityk9 technology package license.
```

The **show platform cerm** command output shows all tunnels in use by SSLVPN.

```
Number of tunnels      225
...
SSLVPN   D      D      225   N/A
```

The **show webvpn session context all** command output shows no or very few active sessions.

```
WebVPN context name: SSL_Context
```

```
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
```

Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq77274

Symptoms: FXS phones are not recognized as SCCP endpoints.

Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

Workaround: There is no workaround.

- CSCtq86500

Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

Workaround: Disable VSA and use software encryption.

- CSCtq86515

Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq91176

Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtq92182

Symptoms: An eBGP session is not established.

Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtr26373

Symptoms: The interface bounces, and after coming back up, hangs and does not pass traffic. The Rx ring is stuck and it may be observed that all packets coming into the interface are counted as “input errors”.

Conditions: This symptom has been observed on the Cisco 3900. This issue may be seen at random times and has thus far been observed to happen after an interface bounce. The interface will still show “up/up” in the **show interface** command output.

Workaround: Bounce the interface again to restore service.

- CSCti72131

Symptoms: An additional static route is seen in the routing table.

Conditions: This symptom occurs when you configure a static route with the DHCP option.

Workaround: There is no workaround.

- CSCtr50118

Symptoms: The router crashes.

Conditions: This symptom occurs when the presence feature is turned on.

Workaround: There is no workaround.

- CSCso46409

Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM-VPN/SSL-3.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)T1

Cisco IOS Release 15.1(3)T1 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T1 but may be open in previous Cisco IOS releases.

- CSCtd91542

Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

Conditions: This symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

Workaround: Avoid using the **show ip multicast rpf tracked** command.

Further Problem Description: The **show ip multicast rpf tracked** command is not intended for customer use and is being deprecated.

- CSCtf36402

Symptoms: A Cisco router crashes when the user telnets and Transmission Control Block is cleared for that session before entering the password.

Conditions: This symptom is observed when aaa authentication protocol is set to TACACS.

Workaround: Do not clear the Transmission Control Block for a session before entering the password.

- CSCtf54561

Symptoms: A MPLS TE FRR-enabled router can encounter a crash if the **show ip cef vrf vrf-name** command is issued.

Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

Workaround: The command should not be issued when many topology changes occur on interface flaps.

- CSCtf56107

Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

Conditions: This symptom is observed when an unknown notify message is received.

Workaround: There is no workaround.

- CSCtf71673

Symptoms: A Cisco 10000 series router shows a PRE crash due to memory-corruption with block overrun.

Conditions: This symptom is observed when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in the same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

Workaround: There is no workaround.

- CSCtf72328

Symptoms: BFD IPv4 Static does not fully support AdminDown.

Conditions: This symptom is observed with the following setup and configuration:

Router 1:

```
interface e0/0
ip address 192.168.1.1 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.10.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.2
ip route 10.20.0.0 255.255.0.0 e0/0 192.168.1.2
```

Router 2:

```

interface e0/0
ip address 192.168.1.2 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.20.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.1
ip route 10.10.0.0 255.255.0.0 e0/0 192.168.1.1

interface e0/0
no ip route static bfd e0/0 192.168.1.1

```

Though the BFD state is DOWN, the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtg64175

Symptoms: The ISIS route is missing the P2P link; it is mistakenly marked as “parallel p2p adjacency suppressed”.

Conditions: This symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

Workaround: Do a shut and no shut on the local P2P interface.

- CSCtg72481

Symptoms: Spurious memory access is seen with QoS configurations.

Conditions: This symptom is observed only when sending the traffic for a while.

Workaround: There is no workaround.

- CSCtg73631

Symptoms: Spurious access or crash.

Conditions: EIGRP undergoes a route delete event for a route that is both redistributed and learned as an external. The redistributed route is deleted and external route promoted. An error in the route deletion codepath may result in spurious access or crash.

Workaround: There is no workaround.

Further Problem Description: This issue is not present in Cisco IOS Release 15.0(1)M4.

- CSCtg91572

Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

Workaround: There is no workaround.

- CSCth20696

Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

Conditions: This symptom is observed with Cisco IOS Release 12.4(25c).

Workaround: There is no workaround.

- CSCth37580

Symptoms: Dampening route is present even after removing “bgp dampening”.

Conditions: This symptom is observed under the following conditions:

- DUT connects to RTRA with eBGP + VPNv4.
- eBGP + VPNv4 peer session is established and DUT.
- Also, DUT has VRF (same RD) as the route advertised by RTRA.

In this scenario, when DUT learns the route, it will do the same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

Workaround: There is no workaround.

- CSCth84233

Symptoms: The router may crash due to Redzone memory block corruption (I/O) when “qos pre-classify” is configured under tunnel interfaces. The packet is overwriting the next block.

Conditions: The trigger for this issue is configuring “qos pre-classify”.

Workaround: Remove “qos pre-classify”.

- CSCth93218

Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” is displayed on PfR BR.

Conditions: This symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

Workaround: There is no workaround.

- CSCti22091

Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually re-enabling PfR will not work. A reboot is required.

Conditions: This symptom is observed when PfR is configured with the following conditions:

1. list > application > filter > prefix-list
2. Learn > traffic-class: keys
3. Learn > traffic-class: filter > ACL

Workaround: There is no workaround.

- CSCti25339

Symptoms: A Cisco IOS device may experience a device reload.

Conditions: This symptom occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6.

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2010-3050 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti34396

Symptoms: The router distributes an unreachable next hop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

Conditions: This symptom is observed when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is unreachable.

Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the next hop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
  set ip next-hop <router ip address>
!
router bgp <asn>
  address-family ipv4 vrf <vrf name>
    redistribute static route-map static-nexthop-rewrite
  exit-address-family
  exit
exit
```

Workaround 2: Instead of configuring static routes with a next hop, specify an interface name.

For example, if you had:

```
ip route x.x.x.x 255.255.255.0 y.y.y.y
```

And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

```
ip route x.x.x.x 255.255.255.0 interface serial2/0
```

Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration “set ip next-hop self” is added to route-maps.

When used in conjunction with the newly added configuration:

```
router bgp <asn>
  address-family vpnv4 unicast
    bgp route-map priority
```

The “set ip next-hop self” will override “next-hop unchanged allpaths” for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti50607

Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

Conditions: This symptom is observed on a Cisco 7200 series router with SRE1 code.

Workaround: There is no workaround.

- CSCti51145

Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

Conditions: In order to see this problem, ALL of the following conditions must be met:

- The nonreloading device must have a “neighbor x.x.x.x transport connection-mode passive” configuration, or there must be an ip access list or packet filter that permits connections initiated by the reloading device, but not by the nonreloading device. In Cisco IOS, such ip access-lists typically use the keyword **established** or **eq bgp**.
- It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
- When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
- Both peers must be multisession capable.
- “transport multi-session” must not be configured on either device, or enabled by default on either device.
- “graceful restart” must not be configured.

Workarounds:

1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
3. Configure a very short keepalive interval (such as one second) on the nonreloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down, if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS 12.2(33)SB-based releases if the 12.2(33)SB router is the one not reloading.

- CSCti61949

Symptoms: Unexpected reload with a “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

Conditions: This symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti66076

Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

Condition: This symptom is observed under the following conditions:

- HSRP version 1 is the protocol that must be used.
- Use HSRP with sub-interfaces on ES20 module.
- Reload the ES20 module.

Workaround: Change to HSRPv2, which is not exposed to the issue.

Alternate Workarounds:

1. Reconfigure HSRP on all subinterfaces.
2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti67102

Symptoms: Tunnel disables due to recursive routing loop in the RIB.

Conditions: This symptom is observed when a dynamic tunnel, which by default is passive in nature, is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install the EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

Workaround: There is no workaround.

- CSCti67905

Symptoms: A Cisco router may experience a crash.

Conditions: This has been experienced on Cisco routers running Cisco IOS Release 15.1(2)T and Cisco IOS Release 15.1(2)T1. The routers are configured with IOS firewall and are inspecting FTP packets.

Workaround: There is no workaround.

- CSCti68721

Symptoms: The output of **show performance monitor history interval <all | given #>** will appear to have an extra column part way through the output.

Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

Workaround: If the symptom occurs, repeat the command.

- CSCti75666

Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

Conditions: This symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.

Workaround: Convert H.323 leg to SIP.

- CSCti79848

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>.

- CSCti84762

Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

Conditions: This symptom is observed with peer flaps or route churn and with an interface flap.

Workaround: Do a hard reset of the stuck peers.

- CSCti85446

Symptoms: A next hop static route is not added to RIB even though the next hop IP address is reachable.

Conditions: This symptom is observed with the following conditions:

1. Configure a next hop static route with the **permanent** keyword.
2. Make the next hop IP address unreachable (e.g.: by shutting the corresponding interface).
3. Change the configuration in such a way that next hop is reachable.
4. Configure a new static route through the same next hop IP address used in step 1.

Workaround: Delete all the static routes through the affected next hop and add them back.

- CSCti87502

Symptoms: CP Express does not launch. Blank or garbage characters appear in the browser.

Conditions: This symptom is observed when attempting to launch CP Express.

Workaround: A power cycle fixes the issue temporarily.

- CSCti88897

Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Cisco IOS Release 15.1(2) T1, the **service-policy output QOS_CUST_BASIC_OUT** command disappears when the router is reloaded or power cycled.

Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Cisco IOS Release 15.1(2)T1.

Workaround: There is no workaround.

- CSCti91036

Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Cisco IOS Release 15.1(2)T.

Conditions: This symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Cisco IOS Release 15.1(2)T.

- CSCti98219

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

Workaround: There is no workaround.

- CSCtj00039

Symptoms: Some prefixes are in the PE router EIGRP topology although those routes are not being passed to the CE router.

Conditions: This symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj05198

Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

Conditions: This symptom is observed when there are two EIGRP router processes.

Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07885

Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

Workaround:

1. Configure CME-as-SRST with “srst mode auto-provision all”.
2. Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:
 - Stop the MIB on the NMS device that is doing the polling.
 - Turn off SNMP polling on the device.
 - Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj07904

Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

Conditions: This symptom is observed when “no passive interface” is configured.

Workaround: Do not configure “passive-interface default” and allow the interface to be nonpassive by default. Configure “passive-interface <interface>” for the interface to be passive.

- CSCtj08533

Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

Conditions: This symptom is observed when there are redundant paths to the CPE.

Workaround: Use only one path between PE and CPE.

- CSCtj15798

Symptoms: Some modems in PVDM2-xxDM module are marked as BAD after running clean for few days. The **show modem** command will report a “B” in front of the modem (“B - Modem is marked bad and cannot be used for taking calls”).

Conditions: This symptom is observed with the PVDM2-xxDM module.

Workaround: Reloading the router gives another few days of clean connections before the issue comes back again.

- CSCtj17545

Symptoms: Immediately after a switchover, the restarting speaker sends TCP-FIN to the receiving speaker, when the receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

Conditions: This symptom can occur when a lot of BGP peers are established on different interfaces.

Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

```
template peer-session ce-v4
  transport connection-mode passive
```

- CSCtj20163

Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

Conditions: This symptom is observed with the following conditions:

1. Execute **show mpls mldp database**.
2. Reload Encap PE.
3. Crash seen on P router when MLDP neighbors go down.

Workaround: There is no workaround.

- CSCtj21696

Symptoms: The virtual access interface remains down/down after an upgrade and reload.

Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv
NAME: "chassis", DESCR: "2801 chassis" PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF

NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet" PID: CISCO2801 ,
VID: V04 , SN: FOC11456KMY

NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard" PID:
VIC2-2E/M= , VID: V , SN: FOC081724XB

NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch" PID: HWIC-4ESW , VID: V01 , SN:
FOC11223LMB
```

NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire" PID:
WIC-1DSU-56K4= , VID: 1.0, SN: 33187011

NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capacity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB

Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

Symptoms: The following traceback is observed when **clear ip bgp *** is done:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data
5905A0A8 chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP
Scanner", ipl= 0, pid= 549
with call stack
0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
0x403A4E84:bgp_scanner(0x403a4c50)+0x234
```

Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

```
Router# show ip bgp sum
BGP router identifier 10.0.0.1, local AS number 65000
BGP table version is 1228001, main routing table version 1228001 604000
network entries using 106304000 bytes of memory
604000 path entries using 31408000 bytes of memory
762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

The **clear ip bgp *** command is not a very common operation in production network.

Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj27251

Symptoms: A router may crash when modifying a QoS class-map.

Conditions: This symptom is observed when modifying a QoS class-map which is being referenced by two or more policy-maps while traffic is matching the class-map and traversing the router.

Workaround: Remove the policy-maps that match the class-map to be modified by issuing **no service-policy input/output *policy-map name***, make changes to the class-map, and then re-apply the policy-maps by issuing **service-policy input/output *policy-map name***.

- CSCtj28747

Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: This symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj39558

Symptoms: Subinterface queue depth cannot be configured.

Conditions: This symptom is observed when the policy is attached to ethernet subinterfaces.

Workaround: There is no workaround.

- CSCtj40564

Symptoms: The Cisco ASR 1000 router disallows an incoming Internet Key Exchange (IKE) connection that matches a keyring. This issue occurs after the router is reloaded.

Conditions: This symptom occurs when a crypto keyring, which has a local-address defined as an interface, is used.

```
crypto keyring keyring_test
pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
local address Loopback2104
```

Workaround: Use an IP address.

```
crypto keyring keyring_test
pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
local address <ip address>
```

- CSCtj41194

Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6>

- CSCtj47736

Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

Conditions: This symptom is observed when the neighbor is learned. Then, you add a max-service limit on an address family. Then, do a shut/no shut on the interface.

Workaround: There is no workaround.

- CSCtj48629

Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

Conditions: This symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtj52077

Symptoms: The policy at the subinterface is not accepted with CBWFQ.

Conditions: This symptom is observed when the policy is used in the Ethernet subinterface.

Workaround: There is no workaround.

- CSCtj58943

Symptoms: The standby RP reloads due to line-by-line sync failure for the **encapsulation dot1q 1381** command:

```
Config Sync: Line-by-Line sync verifying failure on command:
encap dot1Q 1381
due to parser return error
```

rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync,
Reason: Configuration mismatch

Conditions: This symptom occurs when issuing a configuration command under a subinterface mode.

Workaround: There is no workaround.

- CSCtj65553

Symptoms: The static route that is installed in default table is missing.

Conditions: The static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on the Cisco Catalyst 3000 series switching module.

Workaround: Configure the missing static route.

- CSCtj66235

Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

```
%SYS-6-STACKLOW: Stack for process voice
file acct dump running low, 0/6000
```

Conditions: The crash suggests that the issue is just one of inefficient stack usage.

Workaround: There is no workaround.

- CSCtj67845

Symptoms: A Cisco 2951 router crashes on power up.

Conditions: This symptom is observed on a Cisco 2951 router when an HWIC-ADSL and EHWIC-VA-DSL are plugged in together.

Workaround: There is no workaround.

- CSCtj68636

Symptoms: WAAS_Express trial license is missing in Cisco IOS universalk9_npe image for Cisco 880 and 890 platforms.

Conditions: This symptom occurs while using the WAAS Express trial license.

Workaround: Install the Cisco IOS WAAS Express permanent license.

- CSCtj69886

Symptoms: NTP multicast over multiple hops.

Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

Workaround: There is no workaround.

- CSCtj77004

Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

Conditions: The symptom is observed when “archive log config” is configured.

Workaround: There is no workaround.

- CSCtj77477

Symptom: High delay in priority queue when using CBWFQ/LLQ.

For example: EFM rate 2304 kbps

```
888E Average delay: 42ms
888E Max delay: 63ms
HWIC-4SHDSL-E Average delay: 216ms
HWIC-4SHDSL-E Max delay: 361ms
```

Conditions: This symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

Workaround: Configure hierarchical QoS on the WAN G.SHDSL EFM interface.

For example: EFM rate 2304 kbps

```
policy-map CHILD
  class voice
    priority percent 25
  class business
    bandwidth percent 50
policy-map PARENT
  class class-default
    shape average 2100000 8400 0
  service-policy CHILD
```

- CSCtj77963

Symptoms: Resets are observed on low-speed links.

Conditions: This symptom is observed on low-speed interfaces over the WAN that produce retransmissions, out of order segments, etc.

Workaround: There is no workaround.

- CSCtj78210

Symptoms: One-way audio. Moves from one port to another when the router is rebooted.

Conditions: The symptom is observed when using multiple “session protocol multicast”, “connection trunk” configurations for LMR, E&M Immediate, and/or other multicast applications, such as the conditions where this was first detected, in a Radio over IP solution. This symptom only affects PVDm3.

Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

For example, perform the following configurations:

```
voice-card 0 (1... 2... etc...)
dspfarm
dsp service dspfarm

dspfarm profile x conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x2 conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x3 conf
max sessions xx << use maximum (if allowed)
max partic << use the maximum (if allowed)
```

```

associate app sccp
no shutdown

dspfarm profile x conf
shutdown
no dspfarm profile x conf

```

The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- CSCtj81533

Symptoms: The following error message is seen:

```
np_vsmgr_modify_connection: invalid service id 11 passed
```

No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

Workaround: There is no workaround.

- CSCtj82292

Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

Conditions: This issue occurs when summary address is advertised as follows:

```
ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
```

Workaround: There is no workaround.

- CSCtj84901

Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU, when a PVDM module is present in the router.

Conditions: This symptom is observed on Cisco 1900 series, 2911, and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The following modules currently connect to MGF:

1. Service Ready Engine modules (ISM and SM SRE).
2. EtherSwitch modules (SM and EHWIC).

If any traffic from these modules flows over the MGF port towards the router CPU, then the router crashes.

This symptom is not observed on Cisco 2951, 3900 series, or 3900e series routers.

Workaround: For the EHWIC EtherSwitch module with PVDM on the router, there is no workaround.

For the EtherSwitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj85333

Symptoms: System may crash when config-template contains the config command **ip ips signature-category** and when the template is downloaded to the router using the CNS configuration feature using the **cns config retrieve** EXEC command and the **cns config initial** configuration command. This symptom may also occur when the configuration template is downloaded to the router using the device config-update operation of the configuration engine.

Conditions: This is normal mode operation, but this symptom will occur when any such CNS features are used.

Workaround: There is no workaround.

- CSCtj87180

Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

Conditions: This symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multi-hop peer.

Workaround: There is no workaround.

- CSCtj89941

Symptoms: IOSd crash occurs when using the command **clear crypto session** on an EzVPN client.

Conditions: This symptom is observed with the following test bed setup:

1. RP2+ESP20 working as the EzVPN simulator, which is configured with over 1000 clients. Then the simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured.
2. Use IXIA to generate 1 Gbps traffic.
3. Wait until all the SAs have been established and traffic is stable.
4. Use CLI **clear crypto session** on EzVPN simulator.

Workaround: There is no workaround.

- CSCtj90438

Symptoms: Router crashes if “no switchport” is executed on /1 interface of Enhanced EtherSwitch (ESW) or Service Ready Engine (SRE) module.

Conditions: This symptom occurs while executing “no switchport” on the /1 interface of ESW or SRE module without HWIC-4ESW, HWIC-D-9ESW, HWIC-4ESW-POE, HWIC-D-9ESW-POE, NM-16ESW, and NM-16ESW-1GIG present.

Workaround: Do not execute the **no switchport** command on the above mentioned modules as this command does not apply to these modules.

- CSCtj91764

Symptoms: A Cisco UC560 or UC540 platform that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to the CPU.

Conditions: This symptom occurs during a complete SNMP MIB walk.

Workaround: Exclude the CISCO-CALL-APPLICATION-MIB via configuration.

- CSCtj94297

Symptoms: “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

Workaround: Use the **clear ip mroute** command in the affected mroute.

- CSCtk02647

Symptoms: On an LNS that is configured for L2TP aggregation, per-user ACLs downloaded via Radius may cause PPP negotiation failures (IPCP is blocked).

Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL is downloaded for PPP users via radius.

Workaround: There is no workaround.

- CSCtk06548

Symptoms: Using CCBU CVP solution, SIP calls are disconnected during stress test.

Conditions: This symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by SIP stack. It is seen with PI14 image testing.

Workaround: Use PI12 image.

Further Problem Description: The fundamental issue involves the selective ack (SACK) feature. An alternative workaround would be to disable the “SACK Permitted” option from the peer.

- CSCtk12608

Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

Conditions: These symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T, and 15.1(01)S and with the following configurations:

```
Router 1:
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.0.1 remote-as 200
 neighbor 172.16.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 10.10.200.1
ip route 172.16.0.1 255.255.255.255 10.0.12.2
ip route 172.16.0.1 255.255.255.255 10.0.120.2

Router 2:
interface Loopback200
 ip address 10.10.200.1 255.255.255.0
!
interface Loopback201
 ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!
interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
```

```

!
router bgp 200
  no synchronization
  bgp log-neighbor-changes
  network 10.10.200.0
  neighbor 10.0.12.1 remote-as 100
  neighbor 10.0.12.1 update-source Loopback201
  no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!

```

Workaround: Use static routes tied to a specific interfaces instead of using floating static routes.

- CSCtk35953

Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

Conditions: The symptom is observed only if DUT has eBGP-VPNv4 session with a peer and a same-RD is imported on the DUT for the route learned from VPNv4 peer.

Workaround: A hard reset of the session removes the dampening information.

- CSCtk46363

Symptom: A device running Cisco IOS and acting as a DHCP server crashes.

Conditions: This symptom is observed when a client requests a specific IP address.

Workaround: Disable duplicate address detection check using the **ip dhcp ping packet 0** command.

- CSCtk47891

Symptoms: If Fast Reroute (FRR) is in use, the traffic might be blackholed when LC is reset.

Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

Workaround: There is no workaround.

- CSCtk52599

Symptoms: A Cisco 888E router does not train up with a third-party vendor's DSLAM.

Conditions: The symptom is observed when the DSLAM is running new firmware.

Workaround: There is no workaround.

- CSCtk53130

Symptoms: You may be unable to configure **pseudowire** on a virtual PPP interface. The command is rejected with the following error:

```
Incompatible with ipv6 command on Vp1 - command rejected.
```

Conditions: This symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

Workaround: There is no workaround.

- CSCtk53534

Symptoms: Router crashes.

Conditions: The symptom is observed with some combination of zone-based firewall and policy configuration, and with IPv6 traffic.

Workaround: Disable global parameter-map.

- CSCtk56570

Symptoms: When there are some call loads on CUBE, after sending SIP CANCEL, one-way call occurs while call proceeding.

Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

Workaround: Disable media transcoder-high-density.

- CSCtk56817

Symptoms: Router crashes.

Conditions: The symptom is observed when pinging the dialer interface attached to the ATM interface.

Workaround: There is no workaround.

- CSCtk58732

Symptoms: The router may crash if the following configuration is applied:

```
ip sla 1
icmp-jitter 192.0.2.1 source-ip 192.0.2.2 num-packets 1 interval 10
threshold 1000
timeout 1000
frequency 10
ip sla schedule 1 start-time now life forever
track 1 ip sla 1 reachability
```

The following error message is displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 10:49:31 UTC Mon Feb 21 2011 addr=0x1,
pc=0x62D97F30z , ra=0x62D98848z , sp=0x67CE34D0
10:49:31 UTC Mon Feb 21 2011: Address Error (store) exception, CPU signal 10, PC =
0x62DA2E10
```

Conditions: This symptom occurs in Cisco IOS Release 15.1(3)T release. The router may continually reload following the crash.

Workaround: Use the ICMP Echo operation instead, as shown below:

```
ip sla 1
icmp-echo 192.0.2.1 source-ip 192.0.2.2
threshold 1000
timeout 1000
frequency 10
```

- CSCtk61069

Symptoms: The Cisco IOS router crashes.

Conditions: This symptom occurs while using the **write memory** or **show running configuration** commands on the router, after configuring “privilege exec level 15 show adjacency”.

Workaround: Do not set the privilege EXEC level for any form of the **show adjacency** command.

- CSCtk62247

Symptoms: IKEv2 session fails to come up with RSA sign authentication.

Conditions: The symptom is observed with a hierarchical CA server structure.

Workaround: Use non-hierarchical CA servers.

- CSCtk67709

Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

```
ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432- k9.pkg
SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
```

Conditions: This symptom is observed with AnyConnect 3.0.

Workaround: There is no workaround.

- CSCtk74970

Symptoms: TE autoroute-announced tunnel is not installed in the routing table.

Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute-announced tunnel is not installed in the routing table.

Workaround: Configure **no ip routing protocol purge interface**.

- CSCtk84116

Symptoms: A GETVPN KS crash may occur when split-and-merge is happening between the key servers.

Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

Workaround: There is no workaround.

- CSCtk95992

Symptoms: DLSw circuits do not come up when using peer-on-demand peers.

Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

Workaround: Configure the command **dls w udp-disable**.

Further Problem Description: This symptom occurs in Cisco IOS Releases 12.4(15)T14, 12.4(24)T4, 15.0(1)M3, 15.1(1)S, 15.1(2)T, 12.2(33)SX14, 12.2(33)SX14a, and later releases.

- CSCtk96229

Symptoms: Traceback occurs during reloading of the Cisco EtherSwitch module. Looping TCP packets are generated for the active session that exists between the router and switch module in the same router.

Conditions: This symptom is observed when the Cisco EtherSwitch module reloads after you enter the switch module using the **service-module interface** command from the router.

Workaround: There is no workaround.

- CSCtl02057

Symptoms: Router crashes for ATM traffic with multiple GG cards.

Conditions: This symptom occurs when both ATM and PTM modes are present in the router.

Workaround: There is no workaround.

- CSCtl04285

Symptoms: After a BGP flap or while provisioning a new session, the BGP route reflector will not advertise new IPv4 MDT routes to PEs.

Conditions: This symptom is observed with BGP session flap or while provisioning a new session.

Workaround: Enter the **clear ip bgp *** command.

- CSCtl05941

Symptoms: CUBE crashes.

Conditions: This symptom is observed when voice HA is configured on CUBE.

Workaround: There is no workaround.

- CSCtl08014

Symptoms: Router crashes with memory corruption symptoms.

Conditions: This symptom occurs while MLP sessions are initiating, when performing switchover or Online Insertion and Removal (OIR).

Workaround: There is no workaround.

- CSCtl08594

Symptoms: After upgrading to Cisco IOS Release 15.1(3)T, routers are not able to connect to the EZVPN server anymore. ISAKMP fails to find the key.

Conditions: This symptom occurs with the following conditions:

- DHCP is configured on outside interface.
- Outside interface is FastEthernet.

This symptom does not occur if the outside interface is VLAN. This symptom is not seen in Cisco IOS Release 15.1(2)T1.

Workaround: Downgrade to 15.1(2)T1, use VLAN interface, or remove “ip route 0.0.0.0 0.0.0.0 fastethernet4 dhcp” statement from the config and reload the router.

- CSCtl21695

Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million.

Debug vpdn l2x ev/er shows:

```
PPTP _____: TCP connect reqd from 0.0.0.0:49257
PPTP _____: PPTP, no cc in l2x
```

Conditions: This symptom occurs when the LNS is configured for PPTP aggregation and over one millions tunnels have been accepted on VPDN level.

Workaround: Reload LNS.

- CSCtl21884

Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent, even though the static route goes down.

Conditions: The symptom is observed under the following conditions:

- Enable auto-summary under the BGP process.
- Static route is brought into the BGP table via the **network** command.

Workaround: Use the **clear ip bgp *** command or disable auto-summary under the BGP process.

- CSCtl44103

Symptoms: The router crashes when Cisco 3945 router that is running Cisco IOS Release 15.1(3)T, has a zone-based firewall configured.

Conditions: This symptom occurs when using any of the following three debug commands:

- **debug policy-map type inspect events**
- **debug policy-firewall events**
- **debug ip inspect events**

Workaround: There is no workaround.

- CSCtl47666

Symptom: Intermittent call drops for CME SNR calls that go to voicemail.

Conditions: This symptom is observed on a Cisco IP phone with SNR configured. When the “no answer” timer is reached, the call will intermittently drop, instead of going to voicemail.

Workaround: There is no workaround.

- CSCtl50815

Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

```
%OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
Non-OER, OOP Reason <reason>
```

Conditions: The symptom is observed while using the following:

- ECMP
- **mode monitor passive**

Workaround: Remove equal cost routing. For instance, if you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly, as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl57055

Symptoms: A router may unexpectedly reload when the “rttMonStatsTotalsEntry” MIB is polled by SNMP.

Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release. This symptom occurs when the router is configured for SNMP polling and the “rttMonStatsTotalsEntry” is polled with an IP SLA probe configured.

Workaround 1: Configure NMS to stop polling the “rttMonStatsTotalsEntry” or create a view and block the MIB on the router.

Workaround 2: The issue only affects Cisco IOS 15.1T releases, so use a Cisco IOS 15.0(1)M rebuild or earlier.

- CSCtl67195

Symptoms: The following three BGP debug commands cannot be enabled:

- **debug ip bgp vpnv4 unicast**
- **debug ip bgp vpnv6 unicast**
- **debug ip bgp ipv6 unicast**

Conditions: This symptom is observed with the above BGP debug commands.

Workaround: There is no workaround.

- CSCtl71478

Symptoms: In an HA system, the following error message is displayed on the standby RP and LC:

```
OCE-DFC4-3-GENERAL: MPLS lookup unexpected
```

Conditions: This symptom is observed on standby or LC modules, when you bring up both the RP and standby/LC routers with or without any configuration.

Workaround: There is no workaround.

- CSCtl73914

Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

Conditions: The symptom is observed if the “P-Associated-URI of the 200 Ok” response contains any special characters (!*!) in Tel URI Parsing.

Workaround: There is no workaround.

- CSCtl77735

Symptoms: Saving a configuration to NVRAM may fail.

Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

Workaround: Erasing the startup configuration and saving again may recover the configuration.

- CSCtl87879

Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

Workaround: There is no workaround.

- CSCtl88066

Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

Conditions: This symptom is observed when BGP is configured and you issue one of the following commands:

- **show ip bgp all attr nexthop**
- **show ip bgp all attr nexthop rib-filter**

Workaround: Do not issue either of these commands with the “all” keyword. Instead, issue the address family-specific version of the command for the address family you are interested in.

For example, the following are safe:

- **show ip bgp ipv4 unicast attr nexthop**
- **show ip bgp attr nexthop**
- **show ip bgp vpnv4 vrf *vrfname* attr nexthop**

Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing and where this fix is not integrated, are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl92014

Symptoms: After a reprompt element, “enumerate”, using internal variables like `_prompt` or `_dmtof`, no longer produces a valid list of options and repeats the last option.

Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T and later releases.

Workaround: There is no workaround.

- CSCtl98270

Symptoms: Changing the VC hold-queue under PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

Conditions: The symptom is observed in Cisco IOS Release 15.1(2)T2 and later releases.

Workaround: Execute a shut/no shut to fix the issue.

- CSCtn01832

Symptoms: The following command sequence crashes the router at check syntax mode:

config check syntax

route-map hello

match local-preference

no match local-preference

Conditions: The symptom is observed with the above command sequence.

Workaround: There is no workaround.

- CSCtn08613

Symptoms: Cisco router crashes when interfacing with UCCX.

Conditions: This has been experienced when making consult transfer calls on a Cisco UC560 platform that is running Cisco IOS Release 15.1(2)T2.

Workaround: There is no workaround.

- CSCtn09135

Symptoms: MC5728V modem is not enumerated resulting in cellular interface not coming up.

Conditions: This symptom occurs more often with USB flash attached and on DSL SKUs.

Workaround: Removing the USB flash solves the issue in some instances.

- CSCtn27599

Symptoms: The OIR of NM-1T3/E3 line card crashes the router.

Conditions: This symptom is observed only on the Cisco 3945 router.

Workaround: There is no workaround.

- CSCtn51740

Symptoms: Memory leak is seen in the EzVPN process.

Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

Workaround: There is no workaround.

- CSCtn63325

Symptoms: The Cisco 1841 router crashes during firmware upgrade.

Conditions: This symptom occurs when microcode CLI is used during firmware upgrade on the Cisco 1841 router.

Workaround: There is no workaround.

- CSCto88686

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>.

Open Caveats—Cisco IOS Release 15.1(3)T

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(3)T. All the caveats listed in this section are open in Cisco IOS Release 15.1(3)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsr89078

Symptoms: A Cisco AS5400XM reloads unexpectedly on stress with high CPS voice calls and with H.323, g729r8, no VAD and limited DSPs.

Conditions: The symptom is seen only when DSPs on a Cisco AS5400XM are less than the number of calls it can accommodate.

Workaround: Have sufficient available DSPs.

- CSCsz05848

Symptoms: High CPU utilization for DHCP client process.

Conditions: The symptom is observed when 10k PDPs sessions are established.

Workaround: There is no workaround.

- CSCsz97091

Symptoms: Packet drop occurs when **show version**, **show run**, and **write memory** commands are issued.

Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.

Workaround: There is no workaround.

- CSCta40972

Symptoms: The router produces the following message:

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (8/4), process = BGP Router.
```

followed by a traceback, and then both active and standby reload.

Conditions: The symptom is observed when BGP is configured, and then “neighbor x.x.x.x ... prefix-list ...” is configured. This is known to happen at scale when many neighbors are configured, but the exact trigger conditions are not known.

Workaround: Do not enter this CLI for a neighbor in an update-group with lots of other neighbors.

- CSCtb70595
Symptoms: A Cisco router may experience a crash.
Conditions: The symptom is observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(25a).
Workaround: There is no workaround.
- CSCtd42628
Symptoms: Router reloads due to bus error following tunnel flaps.
Conditions: The symptom is observed following tunnel flaps.
Workaround: There is no workaround.
- CSCtd90030
Symptoms: A Cisco 2851 router may crash with a bus error.
Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.
Workaround: There is no workaround.
- CSCtd91542
Symptoms: The **show ip multicast rpf tracked** command may cause a crash.
Conditions: The symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.
Workaround: Avoid using the **show ip multicast rpf tracked** command.
Further Problem Description: The command **show ip multicast rpf tracked** is not intended for customer use and is being deprecated.
- CSCte50870
Symptoms: A Cisco AS5400 crashes due to a watchdog timeout. CPU hogs due to the “SERIAL A’detect” process are seen before the reload:

```
%SYS-3-CPUHOG: Task is running for (36000)msecs, more than (2000)msecs (36/6),process = SERIAL A'detect.
```


After some time the device crashes:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SERIAL A'detect.
```


Conditions: The symptom is seen on a Cisco AS5400 that is running Cisco IOS Release 12.4(24)T2. The serial interfaces of the device are configured with “autodetect encapsulation xxx” and router system clock has been updated:

```
%SYS-6-CLOCKUPDATE: System clock has been updated from 10:42:09 UTC Wed May 19 2010 to 11:42:09 MET Wed May 19 2010, configured from console by console. %SYS-6-CLOCKUPDATE: System clock has been updated from 11:42:09 MET Wed May 19 2010 to 12:42:09 MET-DST Wed May 19 2010, configured from console by console.
```


Workaround: If possible, remove this command.
- CSCte94221
Symptoms: PPP connection over CDMA link is flapping.
Conditions: The symptom is observed when using Cisco IOS Release 15.0M.
Workaround: Shut / no shut the interface and wait for 2 mins.

- CSCtf72156

Symptoms: When the ISDN phone makes a call to a PSTN phone which is switched off, no announcements are heard at the ISDN end.

Conditions: The symptom is observed with a Cisco AS5400 but is independent of the IOS version on the router. There are no other specific conditions.

Workaround: There is no workaround.

- CSCtg13009

Symptoms: DSP crash due to heart beat error. Logs show the following output:

```
%MSDSPRM-3-DSPCRASH: slot 3 dspId 3 heartBeat 022C9632 heartBeatError 1
%MSDSPRM-3-DSPCRASH: slot 3 dspId 2 heartBeat 031FD34B heartBeatError
1coil_show_controller
```

The DSP reset causes no-way audio on conference adhoc or meet me bridge.

Conditions: The symptom occurs during normal operations of ad-hoc and meet-me conferencing.

Workaround: There is no workaround.

- CSCtg42271

Symptoms: A router that is running Cisco IOS Release 15.0(1)M1 may experience a series of spurious memory access errors and a bus error when configured for IPS:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0XXXXXXXXX reading 0XXX
%ALIGN-3-TRACE: -Traceback= 0XXXXXXXXX 0XXXXXXXXX 0XXXXXXXXX 0XXXXXXXXX 0XXXXXXXXX
0XXXXXXXXX
%ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
ra=0xFFFFF3331z , sp=0x28F88EB0
%ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
ra=0xFFFFF3331z , sp=0x28F88EB0
XX:XX:XX XXX XXX XX XXXX: TLB (store) exception, CPU signal 10, PC = 0XXXXXXXXX
```

Conditions: The symptom is observed when the device is configured for IPS and is running Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

- CSCtg47129

The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat>

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtg67146

Symptoms: File transfer to the flash fails with a “TF I/O failed in data-in phase” message. Archive command fails 100% of the time whereas a copy command is successful sometimes.

Conditions: The symptom is observed when the router is running Cisco IOS Release 12.4(24)T or above and has a STI flash 7.2.0. The transfer fails with some delay (~50-100msec).

Workarounds:

1. Transfer without a delay.
2. Transfer with Cisco IOS Release 12.4(9)T.
3. Transfer with a newer flash card.

Further Problem Description: Issue is seen with Cisco IOS Releases 12.4(24)T, 12.4(24)T1, 12.4(24)T2, 12.4(24)T3, and 15.1(1)T.

- CSCtg67346

Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show “Di1 DDR: dialer_fsm_pending() di1”.

Conditions: The conditions are unknown at this time.

Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCtg68568

Symptoms: A Cisco 3945 router configured as a GETVPN group member might crash when passing traffic.

Conditions: The symptom occurs when fragmentation of the IP datagram is required due to MTU limit of 1500 bytes.

Workaround: Configure hosts to negotiate lower TCP MSS (1360) bytes and avoid fragmentation.

- CSCtg72481

Symptoms: Spurious memory access is seen with QoS configurations.

Conditions: The symptom is observed only when sending the traffic for a while.

Workaround: There is no workaround.

- CSCth14305

Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if linkmembers flap as the changes in bandwidth will not be handled correctly.

Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth19516

Symptoms: A router crashes if you have PFR and SAF enabled on the same device.

Conditions: The issue is seen when you have SAF enabled and PFR with multiple links. When the network gets congested or delay is seen and if there is a change over from IN-POLICY state to OOP the router crashes.

Workaround: Disable SAF completely and reload the router.

- CSCth20696

Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

Conditions: The symptom is observed with Cisco IOS Release 12.4(25c).

Workaround: There is no workaround.

- CSCth23354

Symptoms: Packets are not reaching the proper queue.

Conditions: The symptom is observed when class-map is configured with VLAN.

Workaround: There is no workaround.

- CSCth29426

Symptoms: When you issue a **reload** command with a getmany looping on ciscoFlashMIB, the router hangs.

Conditions: The symptom is observed when a getmany is running with only one router. The chances of hitting the issue seem to be increased if a **write memory** has been done before reload or even if the configuration is dirty and you respond “no” to the save configuration prompt.

Workaround: Avoid reloading while doing an SNMP walk on ciscoFlashMIB.

- CSCth37580

Symptoms: Dampening route is present even after removing “bgp dampening”.

Conditions: The symptom is observed under the following conditions:

- DUT connects to RTRA with eBGP + VPNv4.
- eBGP + VPNv4 peer session is established and DUT.
- Also DUT has VRF (same RD) as route advertised by RTRA.

In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

Workaround: There is no workaround.

- CSCth38565

Symptoms: The router crashes after traffic stops and the WE router is unconfigured. This problem is intermittent and very difficult to reproduce.

Conditions: The symptom is observed when the WE is configured for full optimization, traffic is passed and then the WE router is unconfigured. The type of traffic being passed does not seem to affect the crash.

Workaround: There is no workaround.

- CSCth51168

Symptoms: An H.323 to H.323 CUBE may incorrectly reuse existing TCP sockets when completing H.323 calls. This leads to call failures with cause values of:

18 - No user responding
or

102 - Recovery on timer expiry

Conditions: The symptom is observed on a Cisco 7206VXR CUBE handling 100+ calls with Cisco IOS Release 12.4(22)T5.

Workaround: Disable reuse of TCP sockets with the following commands:

voice service voip

h323

h225 timeout tcp call-idle value 0

session transport tcp calls-per-connection 1

- CSCth62136
 Symptoms: The ISDN L2 goes to “Layer 2 NOT Activated.”
 Conditions: This symptom is observed when a service policy is attached to the dialer interface.
 Workaround: Remove the service policy from the interface.
 Further Problem Description: This symptom is not seen with:
 - 12.4(13d)
 - 12.4(15)T12
 This symptom has been seen with:
 - 12.4(22)T5
 - 12.4(24)T3
 - 15.0(1)M3
- CSCth64316
 Symptoms: Unable to configure “radius-server” using SNMP set.
 Conditions: The symptom is observed when you configure via SNMP MIB.
 Workaround: Radius server can be configured through the CLI.
- CSCth66604
 Symptoms: ISSU incompatibility due to different versions of a protocol (NTP v3 and NTP v4).
 Conditions: The symptom is observed with an ISSU upgrade or downgrade.
 Workaround: Unconfigure the CLIs causing MCL errors and repeat the ISSU process again.
- CSCth68038
 Symptoms: After a simulated failover of an L2L tunnel, a Cisco 7200 series router with VSA will fail to encrypt traffic for a period of time, typically for several minutes. VSA will then begin to encrypt traffic correctly.
 Conditions: The problem appears to be triggered when manually failing over a spoke from one hub Cisco 7200 (without VSA) to a secondary hub Cisco 7200 with VSA. The issue only affects virtual-template interfaces.
 Workaround: Use software encryption.
- CSCth71648
 Symptoms: G3 fax fails.
 Conditions: The symptom is observed when T38 v3 is configured on gateway and Cisco fax server.
 Workaround: Configure gateway and fax server with T38 V0.
- CSCth77562
 Symptoms: Unable to read vlanTrunkPortEntry.13 object, but can set values to manage VLAN/Trunk mode configuration on NM-ESW16 ports.
 Conditions: The symptom is observed on a Cisco 2800 series router that is running Cisco IOS Release 12.4(24)T3.
 Workaround: There is no workaround.

- CSCth81055

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are not available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ike>

Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCth84233

Symptoms: Router may crash due to Redzone memory block corruption (I/O) when “qos pre-classify” is configured under tunnel interfaces. The packet is overwriting the next block.

Conditions: The trigger for this issue is configuring “qos pre-classify”.

Workaround: Remove “qos pre-classify”.

- CSCth87041

Symptoms: Router hangs.

Conditions: The symptom is observed when unconfiguring “match field” under class map.

Workaround: There is no workaround.

- CSCth87348

Symptoms: Virtual access multilink interface fails to come up.

Conditions: The symptom is observed when “frame-relay traffic-shaping” and O/P service policy are applied, then shut/no shut the interface.

Workaround: There is no workaround.

- CSCth90147

Symptoms: Router will respond to an RS with an RA.

Conditions: The symptom is observed when you configure the command **ipv6 nd ra suppress**. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

Workaround: Use an ACL to block the reception of RS packets.

- CSCth93218

Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

Workaround: There is no workaround.

- CSCti03199

Symptoms: During switch-over, standby crashes after every recovery due to config-sync.

Conditions: The symptom is observed when the standby tries to sync with the active and when “crypto pki trustpoint” is configured with an unavailable port-channel as source-interface.

Workaround: There is no workaround.
- CSCti09284

Symptoms: A Cisco device may display the following error messages in the logs when IPS is enabled:

```
%SYS-2-CHUNKINVALIDHDR: Invalid chunk header type
```

Conditions: The symptom is observed when IPS rulesets are enabled on the interfaces.

Workaround: Remove IPS ruleset configuration from interface configurations.
- CSCti10928

Symptoms: Xcoder sends empty RTP stream in one direction only.

Conditions: The symptom is observed on a CUBE that is running Cisco IOS Release 12.(24)T3 with an incoming fast start call.

Workaround: There is no workaround.
- CSCti13493

Symptoms: A router crashes and the following traceback is seen:

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP",
ipl= 0, pid= 226, -Traceback=
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
```

Conditions: The symptom is observed with the DSMP process.

Workaround: There is no workaround.
- CSCti17841

Symptoms: Removing “match condition” from a class map crashes the router.

Conditions: The symptom is observed when you remove “match condition” from a class map.

Workaround: There is no workaround.
- CSCti19261

Symptoms: A Cisco 87xW router and other routers with a wireless device will crash in rare cases when transmitting a packet.

Conditions: The symptom is observed with normal traffic.

Workaround: There is no workaround.
- CSCti25459

Symptoms: Device might crash with fib_forw_add_extra_encap_and_forward. Also possibly seeing ICMP packets with unreachable sourced.

Conditions: The symptom is observed when MLPS is enabled on these devices.

Workaround: Use NAT NVI instead of legacy NAT.
- CSCti32334

Symptoms: DDNS process gets stuck and marks all updates as duplicates. The command **debug ip dhcp server packet detail** shows:

DDNS: Duplicate update rejected 'host.somedomain.com.' <=> 192.168.0.1 server 0.0.0.0
 Conditions: This happens in a day or so under moderate load following a router reboot. DDNS updates are performed by IOS DHCP server ("update dns" is configured in a pool).

Workaround: There is no workaround.

- CSCti34056

Symptoms: If ISAKMP (P1) SA is lost but a valid IPsec SA (P2) still exists with a constant inbound data traffic being received from the peer, periodic DPD configuration does not re-trigger IKE and hence DPDs are not sent to the peer.

Conditions: Router A and Router B are configured with LAN-to-LAN IPsec tunnel. Router B has "crypto isakmp keepalive 10 3 periodic" configured. Router B loses IKE SA, after which DPDs are not sent.

Workaround: Execute a **clear cry sa** (P2) or **clear cry session** on Route B to reinitiate a new IKE P1.

- CSCti34968

Symptoms: ACL with QoS is crashing the router, if one of the ACEs is evaluate or reflect.

Conditions: The symptom is observed if the pure ACL used under a class-map is also a reflexive ACL. It is observed only in a pure QoS class-map configuration which has only access-group match filter. It is not seen with an impure QoS class-map configuration which has access-group as well as other filters like DSCP.

Workaround: Do not use reflexive ACL under QoS. It is not a good practice.

- CSCti36310

Symptoms: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attribute are pulled by SNMP.

Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprise9.03.01.00.S.150-1.S and asr1000rp1-adventerprise9.02.06.01.122-33.XNF1 images.

Workaround: There is no workaround.

- CSCti47995

Symptoms:

1. Traffic gets punted and dropped since CEF has stale state of prefix.
2. IP complains of duplicate address:

%IP-4-DUPADDR: Duplicate address 192.168.0.101 on FastEthernet1/2, sourced by 0030.7bb9.f01e

Conditions: The symptom is observed when there is NAT configured, traffic is flowing and then NAT is unconfigured.

Workaround: There is no workaround.

- CSCti49372

Symptoms: V.34 modem relay call connects for few seconds, shows a lot of garbage characters on originating and terminating hyperterminals, and then gets disconnected.

Conditions: This is seen with external modems and MGCP gateways configured for V.34 modem relay.

Workaround: There is no workaround.

- CSCti50607
Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.
Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.
Workaround: There is no workaround.
- CSCti54127
Symptoms: System crash.
Conditions: The symptom is observed with the following conditions:
 1. Configure 12-in-1 serial in Async mode.
 2. Launch sweep pings (with incremental packet sizes) from the peer to UUT.
 3. Configure “mtu 64” on serial interface of UUT.
 4. Configure “default mtu” on serial interface of UUT.
 Workaround: Stop traffic or shut down the interface before modifying the MTU configuration.
- CSCti54149
Symptoms: Fax machine sends out v29, signaling proprietary faxing.
Conditions: The symptom is observed when sender and receiver are using same type of fax machine.
Workaround: There is no workaround.
- CSCti54217
Symptoms: Unexpected reload may occur with the following message:

```
Unexpected exception to CPU: vector 1400, PC = 0x803445B8, LR = 0x803385C4
```

 Conditions: The symptom is observed on a Cisco 1812 router that is running Cisco IOS Release 12.4(15)T12.
Workaround: There is no workaround.
- CSCti54671
Symptoms: A SIP REFER sent to CUBE with SIP header Call-Info=<parameter data> is not passed to the outbound INVITE on CUBE. The data in SIP header Call- Info is lost.
Conditions: This symptom is observed in a SIP environment supporting CVP, CUBE, and ICM. ICM sends instructions to CVP to add the Call-Info header to the REFER message. The Call-Info header contains data elements that need to be passed to a target system. CUBE is configured to consume the REFER, thereby generating an INVITE to send to the target system. The REFER process works as expected, i.e.: the INVITE is forwarded to the target system. But the Call-Info data element is lost in the transaction from REFER method to INVITE method.
Workaround: There is no workaround if a REFER is used. However, if CVP sends an re-INVITE with SIP header Call-Info=<parameter data>, CUBE does forward the data element correctly to the target system.
- CSCti56560
Symptoms: With bursty traffic, drops are seen in the interface drop counters that are not accounted for in the per-traffic-class counters. Furthermore, some of these unaccounted packet drops may occur in a traffic-classes where the offered rate is much less than the shape rate (i.e.: where the shaper is not active).
Conditions: The symptom is observed with a hierarchical policy-map with shape in several parent traffic-classes and fair-queue in the child traffic class is applied to a POS interface.

Workaround 1: Set “hold-queue 4096 out” under the interface configuration mode. This will set up a maximal output buffer to make the driver more tolerant of bursts.

Workaround 2: Tune the shaper to eliminate excess bursts.

- CSCti58426

Symptoms: A router may encounter a crash when the **show buffers usage** command is issued.

Conditions: The symptom is triggered by the **show buffers usage** command.

Workaround: Avoid running the **show buffers usage** command.

- CSCti58625

Symptoms: When you issue the command **privilege voiceport level 2 shut** in a configuration terminal, the VG224 will become hung for over two hours. After the command is enabled, it also takes a long time to issue a **write memory** or **show run**.

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T. Other releases may be affected.

Workaround: There is no workaround.

- CSCti59419

Symptoms: Double digits being sent (OOB and RFC2833).

Conditions: The symptoms are observed if no DTMF method is specified in the CRCX from CA and when running Cisco IOS Release 12.4(25c) and above.

Workaround: Use Cisco IOS Release 12.4(7c).

- CSCti59428

Symptoms: TCP sessions stop working after a few days.

Conditions: The symptom is observed when a TCP session has been opened for a long time, e.g.: for TCP SYSLOG use.

Workaround: There is no workaround.

- CSCti59648

Symptoms: Intermittently (approximately once every 4 or 5 calls), ISDN calls are disconnected by the Cisco MGCP gateway.

Conditions: The symptom is observed because the CallManager times out waiting for CONNECT_ACK from the MGCP gateway (i.e.: T313 timer). The gateway does receive CONNECT_ACK from the PSTN almost immediately following the outgoing CONNECT. However, the gateway seems to encounter huge delays in back- hauling the CONNECT_ACK to CallManager.

Workaround: Increase the “T313 timer” service parameter in Cisco Unified Communications Manager Administration page. Note that while this may alleviate the issue, the problem could still happen, perhaps less frequently.

- CSCti62801

Symptoms: When both Caller-ID (CID) and Call-Waiting (CW) features are enabled on SIP analog endpoint, repetitive Call-Waiting (CW) tone is not played every 10 seconds until call is answered.

Conditions: The symptom is observed with a SIP analog endpoint on IAD243x, when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features using SIP for the phone connected to the FXS port.

Workaround: There is no workaround.

- CSCti63640

Symptoms: A Cisco AS5400XM reloads due to:

`%SYS-6-STACKLOW: Stack for process Framer background.`

Conditions: The issue seen with Cisco IOS interim Release 15.1(02.14)T while booting up the router with ds0-group configurations (in startup config) for the controllers that are connected back-to-back in the same router.

Workaround: There is no workaround.

- CSCti66153

Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment is logging the following error:

`%VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Selector checks.`

Conditions: The following conditions need to be met:

- A Cisco 7200 series router with VSA in receive-only mode.
- Keyserver in receive-only mode.
- Other GM in passive mode (that is encrypting outbound traffic) sending traffic to the “inside” of the Cisco 7200.
- Traffic matching a keyserver delivered crypto ACL matching L4 ports (e.g.: **permit tcp any any eq 23**).

Workaround: Relaxing any of the conditions here above:

1. Use VAM2+ instead of VSA.
2. Use GETVPN ACL without l4 ports (e.g.: **permit ip any any**).
3. Have the Cisco 7200 in passive mode as well.
4. Not using receive-only mode on the keyserver.

- CSCti66155

Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67832

Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

Workaround: There is no workaround.

- CSCti67905
Symptoms: A Cisco router may experience a crash.
Conditions: This has been experienced on Cisco routers running Cisco IOS Release 15.1(2)T and Release 15.1(2)T1. The routers are configured with IOS firewall and are inspecting FTP packets.
Workaround: There is no workaround.
- CSCti69990
Symptoms: A router crashes after deconfiguring IPv6 and then reconfiguring.
Conditions: The symptom is observed only under specific conditions. Router has IPv6 configured on a number of interfaces and also has GLBP configured. IPv6 configuration is removed from all interfaces and then re-applied.
Workaround: There is no workaround.
- CSCti71071
Symptoms: The command **show policy-map multipoint** does not show any output on a hub, configured with a per-tunnel-QoS policy on its tunnel interface. The command is also not displayed in the parser options upon issuing **show policy-map ?**.
Conditions: The symptom is observed with the **show policy-map multipoint** command.
Workaround: There is no workaround.
- CSCti75666
Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.
Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.
Workaround: Convert H.323 leg to SIP.
- CSCti77384
Symptoms: Traceback is seen while configuring DHCP on a virtual-template.
Conditions: The symptom occurs during a PPPoE session.
Workaround: There is no workaround.
- CSCti77879
Symptoms: When the traffic to encrypt matches the first sequence of a crypto map, starting its crypto ACL with a deny statement, the traffic is dropped whether or not this deny statement is a subset of the permits contained in that crypto ACL or not.
Also, the limitation of 14 denies in an ACL due to the jump behavior does not seem to be present.
Conditions: The symptom is observed in a VSA installed in a Cisco 7200 series router that is running Cisco IOS Release 15.0(1)M3.
Workaround: There is no workaround.
Further Problem Description: As the configuration guide states, the **crypto ipsec ipv4-deny {jump | clear | drop}** command should help to avoid this problem, but this command is not available for the VSA, only for VPN SPA.
- CSCti79442
Symptoms: One-way voice.

Conditions: The symptom is observed on a Cisco AS5400 MGCP controlled by PGW, SIP to PSTN call, with echo cancellation enabled. You see the RTP RX/TX counters increment with the **show call active voice brief** command.

Workaround: Explicitly define the MGCP codec type: **mgcp codec g711ulaw packetization-period 20**.

- CSCti79696

Symptoms: A Cisco device may reload unexpectedly when a user edits content filtering settings through Cisco Configuration Professional (CCP).

Conditions: The symptom is observed when editing content filtering settings through CCP.

Workaround: Use command line instead of CCP.

- CSCti79848

Symptoms: Router is running out of memory due to Chunk Manager.

Conditions: The conditions are not confirmed at this time. It is believed to be related to Zone-based Firewall.

Workaround: There is no workaround.

- CSCti82141

Symptoms: The following symptoms are observed:

1. The “none” option will be missing in the **show run** output after “ntp pps-discipline none inverted stratum <#value>” is configured.
2. “Invalid input detected” error message will be thrown during the bootup and the configured “ntp pps-discipline none inverted stratum <#value>” will vanish after a reload.

Conditions: The symptom is observed when the “inverted” option is included in the “ntp pps-discipline” CLI.

Workaround: Configure the CLI without the “inverted” option.

- CSCti85446

Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

Conditions: The symptom is observed with the following conditions:

1. Configure a nexthop static route with permanent keyword.
2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
3. Change the configuration in such a way that nexthop is reachable.
4. Configure a new static route through the same nexthop IP address used in step 1.

Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti88897

Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2) T1, the command **service-policy output QOS_CUST_BASIC_OUT** disappears when the router is reloaded or power cycled.

Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2)T1.

Workaround: There is no workaround.

- CSCti89532
Symptoms: Classes in a policy-map are not getting the specified bandwidth for the class.
Conditions: This happens when a bandwidth policy is attached to an ATM interface.
Workaround: There is no workaround.
- CSCti89976
Symptoms: Standalone AnyConnect 3.0 client does not work with an existing IOS headend.
Conditions: The symptom is observed when AnyConnect 3.0 is used with an existing IOS headend.
Workaround: Use client versions less than or equivalent to 2.5, or use weblaunch.
- CSCti91036
Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Release 15.1(2)T.
Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Release 15.1(2)T.
Workaround: There is no workaround.
- CSCti93175
Symptoms: NAT router does not translate address of the last TCP ACK in the 3- way handshake.
Conditions: The symptom is observed with the following conditions:
 - VRF NAT is involved.
 - “ip nat outside source translation” has to exist.
 - NAT flow-entries are disabled by **no ip nat create flow- entries**.
 Workaround: There is no workaround.
- CSCti93208
Symptoms: HWIC-2SHDSL fails to train up with a third party vendor’s DSLAM.
Conditions: This happens only if the board revision of the HWIC is C0.
Workaround: Use a card with the board revision B0.
- CSCti93600
Symptoms: Bus exception error is received due to a corrupted program counter.
Conditions: The symptom is observed when a GigE link that is assigned to a port-channel is cleared and then followed immediately by a **show interface port-channel**.
Workaround: If the **show interface port-channel** is done after the **clear interface** has completed (so that the GigE link is removed from the port-channel then added back in), the crash is not seen. In general, waiting 10 seconds between the **clear** and the **show** commands will avoid the crash.
- CSCti95511
Symptoms: The command **no buffer header permanent** does not restore the default number of header buffers.
Conditions:
 1. Issue is seen only when configuring header/fast switching buffers.
 2. Buffers need to be created for this pool.

Workaround: Configure the buffer CLIs carefully. This issue could be avoided by:

1. Not configuring “buffer header permanent” with a high value when available memory is low.
 2. Not configuring “no buffer header permanent” when the number of buffers in the free list is less than the minimum value.
- CSCti95682

Symptoms: CUBE crashes at sipSPICopySdpInfo if ReINVITE gets rejected for SRTP call.

Conditions: The symptom is observed with the following conditions:

- “srtp fallback” and “fax protocol pass-through g711ulaw” configured on CUBE.
- Initial call establishes with SRTP and g729r8 codec.
- CUBE receives a ReINVITE with RTP, g711ulaw codec and silenceSupp:off to switch to the fax passthru mode.
- CUBE forwards the ReINVITE to the other end.
- The other end rejects the ReINVITE with “488 Not Acceptable Media” error response (could be because fallback to RTP is not enabled or fax passthru is not enabled on the other end).
- CUBE crashes after receiving 488 error response from the other end.

Workaround: Configure uniform fax protocol (T38 or pass-through) and “srtp fallback” on all the gateways.

- CSCti96109

Symptoms: Overall performance reduction on NAT.

Conditions: The symptom is observed when NAT is enabled.

Workaround: Revert to earlier images.

- CSCti96291

Symptoms: AutoQoS-created class-maps get deleted from all policies when “no auto qos voip” is configured on any one DLCI.

Conditions: The issue is seen on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(2.19)T0.1.

Workaround: There is no workaround.

- CSCti97896

Symptoms: A Cisco ISR router with 512MB of memory and iomem set to 25% may crash and hang at bootup.

Conditions: The symptom is observed when booting a Cisco IOS 15.0 image with iomem set at 25% and 512MB of RAM.

Workaround: Do not configure “memory-size iomem 25”. To restore from the hang you will need to physically reload the router, break to rommon, and issue the following rommon command: **iomemset smartinit**. Check that you have smartinit enabled using the rommon command **meminfo** which would show you “Smart Init is enabled”.

- CSCti98550

Symptoms: A Cisco 870 router crashes upon an AnyConnect connection.

Conditions: The symptom is observed on a Cisco 870 that is running Cisco IOS Release 15.1(1)T1. AnyConnect “client certificate authentication” is configured. The crash occurs when using AnyConnect 2.4 on the iPhone.

Workaround: Use username/password for authentication. Make sure “authorization username subjectname commonname” is configured under the trustpoint.

- CSCti99419

Symptoms: An HWIC-1DSU-T1 card is not recognized after a reload.

Conditions: This symptom is observed on an HWIC-1DSU-T1 card after a reload. It occurs only about 1 to 2 percent of the time.

Workaround: Power-cycle the router.

- CSCtj00039

Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using **clear ip route vrf xxx x.x.x.x**.

- CSCtj00728

Symptoms: A router crashes when enabling a DECnet neighbor.

Conditions: The symptom is observed with a DECnet neighbor limit on a single node of 32. If one exceeds 32, the crash is seen.

Workaround: Limit neighbor count to 32.

- CSCtj01087

Symptoms: CUBE advertises last negotiated payload size information in SIP-SDP after the call is held and retrieved. Call Flow: IP-Phone CUCM SIPIPIGWSIPTelco:

1. IP-Phone calls PSTN over SIP trunk and call connects - G729, 40ms payload size is negotiated.
2. P-Phone puts caller on hold, and caller is connected with MOH - G711ulaw, 20ms payload is negotiated.
3. IP-Phone retrieves the call - G279, 20ms payload size is negotiated.

Conditions: The symptom is observed on a Cisco 3945 router with the c3900-universalk9-mz.SPA.151-2.T.bin image. Voice-class codec is being used in Dial- Peer:

```
voice class codec 1
  codec preference 1 g711alaw
  codec preference 2 g711ulaw
  codec preference 3 g729r8 bytes 40

!
!Incoming Dial-Peer
!
!
dial-peer voice 2001 voip
  tone ringback alert-no-PI
  description Incoming from CISCO UCM
  huntstop
  preference 1
  session protocol sipv2
  incoming called-number .
  voice-class codec 1 offer-all
  no voice-class sip asserted-id
  voice-class sip privacy-policy passthru
  voice-class sip early-offer forced
  voice-class sip profiles 1
  dtmf-relay rtp-nte
```

```

no vad
!
!Outgoing Dial-Peer
!
!
dial-peer voice 1001 voip
tone ringback alert-no-PI
description Outgoing to Prosodie
translation-profile outgoing Outgoing_to_PSTN
huntstop
destination-pattern 0T
session protocol sipv2
session target ipv4:10.3.3.10
no voice-class sip asserted-id
voice-class sip privacy-policy passthru
voice-class sip early-offer forced
voice-class sip profiles 1
codec g711alaw
no vad
!

```

Workaround: Remove the voice-class codec and define the codec explicitly:

```

dial-peer voice 2001 voip
no voice-class codec 1 offer-all
codec g729r8 bytes 40 fixed-bytes

```

- CSCtj01235

Symptoms: A crash is seen when running the command **debug crypto isakmp** during ISAKMP profile selection. The crashinfo file shows that the crash is happening during MM_KEY_EXCH as it receives the certificate from the remote peer.

Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 15.0(1)S.

Workaround: There is no workaround.

- CSCtj01278

Symptoms: The **show memory statistics** command show memory leaks:

```

%SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0xyyyyyyyy, alignment 0
Pool: Processor Free: xxxx Cause: Memory fragmentation Alternate Pool: None Free: 0
Cause: No Alternate pool -Process= "Licensing Auto Update Process", ipl= x, pid= xx

```

Conditions: The symptom is observed using the following command with options: **privilege route-map level x**.

Example: **privilege route-map level 10 set extcommunity privilege route-map level 10 set interface**

Workaround: There is no workaround.

- CSCtj02163

Symptoms: DSP is not being released during voice call connection.

Conditions: The symptom is observed with a hair-pin call across two ports in different slots.

Workaround: There is no workaround.

- CSCtj03381

Symptoms: NAT traffic is getting process switched when you configure “nat entry” or you reload the router.

Conditions: The symptom is observed when you enable VRF-aware NAT with the “match-in-vrf” option.

Workaround 1: Reconfigure “ip cef”.

Workaround 2: Do a **clear ip route vrf <vrf> ***.

- CSCtj05198

Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

Conditions: This symptom is observed when there are two EIGRP router processes.

Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07885

Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

Workaround:

1. Configure CME-as-SRST with “srst mode auto-provision all”.
2. Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:
 - a. Stop the MIB on the NMS device that is doing the polling.
 - b. Turn off SNMP polling on the device.
 - c. Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj07904

Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

Conditions: The symptom is observed when “no passive interface” is configured.

Workaround: Do not configure “passive-interface default” and allow the interface to be non-passive by default. Configure “passive-interface <interface>” for the interface to be passive.

- CSCtj08368

Symptoms: Router software crash at process_run_degraded_or_crash.

Conditions: The symptom is observed when the allocated memory block is freed.

Workaround: There is no workaround.

- CSCtj08533

Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

Conditions: The symptom is observed when there are redundant paths to the CPE.

Workaround: Use only one path between PE and CPE.

- CSCtj08869

Symptoms: Router crash seen when LAT is disabled.

Conditions: This is seen on a Cisco 7200 series router loaded with Cisco IOS interim Release 15.1(2.18)T.

Workaround: There is no workaround.

- CSCtj09256

Symptoms: AnyConnect client fails to connect. The following error messages may be seen:

```
Unable to Process Response from server <servername or IP address of gateway>
Connection attempt has failed due to server communication errors. Please retry the
connection
```

Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(24)T4.

Workaround 1: Use the clientless portal to launch AnyConnect.

Workaround 2: Use Cisco IOS Release 12.4(24)T3 or earlier.

- CSCtj10592

Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

Conditions: The symptom is observed with a simple SVTI to DVTI connection.

Workaround: There is no workaround.

- CSCtj11346

Symptoms: VSA IPsec card can not process encrypted data from peer.

Conditions: The symptom is observed when you enable the VSA card.

Workaround 1: Replace the router (third-party equipment) with a Cisco router.

Workaround 2: Disable the VSA with **no crypto engine slot 0**.

- CSCtj11682

Symptoms: An HWIC-3G-CDMA-S modem slows down to 1xRTT speed and does not recover when 1xEVDO service is available.

Conditions: The symptom is observed when 1xEVDO service is interrupted and the modem goes to the 1xRTT service that is available. When 1xEVDO service returns, the modem does not return to the higher rate service.

Workaround: The following EEM script can be utilized as a workaround for the Cisco 880 series of routers that utilize the PCEX cards. It can be modified to work with the 1800 and larger series of routers that utilize the HWIC cards also:

```
event manager applet WA
 event syslog pattern "%SYS-5-RESTART"
 action 1.1 wait 15
 action 1.2 syslog msg "Applying Service-policy to the Async interface"
 action 2.1 cli command "enable"
 action 2.2 cli command "lab"
 action 2.3 cli command "config terminal"
 action 2.4 cli command "int cell 0"
 action 2.5 cli command "service-policy output TEST"
 action 2.6 cli command "end"
 action 2.7 cli command "write memory"
 action 3.1 syslog msg "Service policy has been configured on the Async
 interface"
```

- CSCtj13210

Symptoms: Memory leaks are observed at **ipsec_db_add_gdoi_sa_req** on GETVPN keyserver.

Conditions: This symptom is observed with GETVPN keyserver when a large amount of traffic is sent between GETVPN GMs.

Workaround: There is no workaround.

- CSCtj14738

Symptoms: Router crash. Before the crash we see the following error messages:

```
%ISDN-6-DISCONNECT: Interface Serial0/0/0:4 disconnected from 6406418 , call lasted
1410 seconds
```

```
%ALIGN-1-FATAL: Illegal access to a low address addr=0x244, pc=0x247BE87Cz ,
ra=0x247BE878z , sp=0x3175D388
```

Conditions: The symptom is observed on a Cisco 2911 router that is running the c2900-universalk9-mz.SPA.150-1.M1.bin image.

Workaround: There is no workaround.

- CSCtj15798

Symptoms: Some modems in PVDm2-xxDM module are marked as BAD after running clean for few days. The **show modem** command will report a “B” in front of the modem (“B - Modem is marked bad and cannot be used for taking calls”).

Conditions: The symptom is observed with the PVDm2-xxDM module.

Workaround: Reloading the router gives another few days of clean connections before the issue comes back again.

- CSCtj15884

Symptoms: One-way voice when SRTP is used.

Conditions: The symptom is observed when interworking with PGW.

Workaround: There is no workaround.

- CSCtj16036

Symptoms: A Cisco router may experience a crash due to a watchdog timeout after seeing CPUHOG messages.

Conditions: This has been experienced on a Cisco 7206XR that is running Cisco IOS Release 12.4(24)T3. The router is configured with PPP interfaces.

Workaround: There is no workaround.

- CSCtj16291

Symptoms: Voice router crashes due to memory corruption.

Conditions: The symptom is observed when multiple SIP Register are received. The response causes a Send Error.

Workaround: There is no workaround.

- CSCtj17425

Symptoms: Router configured for SSL VPN crashes.

Conditions: The symptom is observed when SSL VPN is configured.

Workaround: There is no workaround.

- CSCtj18622

Symptoms: The “qos_peruser” feature is not working when it is pushed through AV_Pair by a RADIUS server; either Cisco ACS or a third party vendor’s server.

Conditions: The symptom is observed with non-multilink PPP users.

Workaround: There is no workaround.

- CSCtj20163

Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

Conditions: The symptom is observed with the following conditions:

1. Execute **show mpls mldp database**.
2. Reload Encap PE.
3. Crash seen on P router when MLDP neighbors go down.

Workaround: There is no workaround.

- CSCtj20588

Symptoms: Router hangs and generates crashinfo files upon reboot after removing an access-list used in a class-map via this command: **no ip access-list <name>**. The following error message is logged prior to the crash:

```
%SYS-3-CPUHOG:Task is running for (120004)msecs, more than (2000)msecs
(976/266),process = SNMP ConfCopyProc.
```

Also, spurious access (%ALIGN-3-SPURIOUS) could be seen (without crashing the router) when that command is entered.

Conditions: The symptom is observed on a Cisco 3845 router after upgrading to Cisco IOS Release 15.1(2)T1.

Workaround: Avoid removing access-lists.

- CSCtj20634

Symptoms: Normal door not getting created.

Conditions: The symptom is observed while sending H225 packets across UUT.

Workaround: There is no workaround.

- CSCtj21045

Symptoms: Header compression decodes RTP timestamp incorrectly.

Conditions: This issue occurs mainly with IPHC format compression interacting with older IOS releases.

Workaround: Use IETF format compression.

- CSCtj21120

Symptoms: CPUHOG for process "IP SLAs XOS Event Processor" is seen followed by a router crash. After the router is reloaded, it then crashes again with the same decode.

Conditions: The symptom is observed when the router is configured with two external interfaces with total of 3200 appls prefix with 50 OER maps and 64 appls prefix in each OER map in fast mode.

Workaround: There is no workaround.

- CSCtj21327

Symptoms: IP addresses are getting NATed properly, but the content-length is not being changed and the resulting packets are rejected by a firewall (due to the content length not being updated).

Conditions: The NAT router is a Cisco 2921 router running Cisco IOS Release 15.0(1)M1 and doing static NAT and NATTING for embedded addresses in SIP packets.

Workaround: There is no workaround

- CSCtj21696

Symptoms: The virtual access interface remains down/down after an upgrade and reload.

Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
OMHQ-C2800-49#sho inv
NAME: "chassis", DESCR: "2801 chassis"
PID: CISCO2801          , VID: V04 , SN: FTX1149Y0KF

NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet"
PID: CISCO2801          , VID: V04 , SN: FOC11456KMY

NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface
daughtercard"
PID: VIC2-2E/M=        , VID: V   , SN: FOC081724XB

NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch"
PID: HWIC-4ESW         , VID: V01 , SN: FOC11223LMB

NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire"
PID: WIC-1DSU-56K4=    , VID: 1.0 , SN: 33187011

NAME: "PVDM 1", DESCR: "PVDMMII DSP SIMM with one DSP with half channel
capacity"
PID: PVDM2-8           , VID: NA   , SN: FOC09123CTB

Workaround: Do a shut/no shut the serial interface.
```

- CSCtj23189

Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.

Conditions: This happens only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with 3 classes: one with 16kbps, second one with 1Mbps, and the third one with 99Mbps.

Workaround: There is no workaround.

- CSCtj28747

Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj32914

Symptoms: CU is getting an error message, spurious memory access, and traceback:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x801697CCz reading 0x0
```

Conditions: The symptom is observed on a Cisco 1861-UC-2BRI-K9 that is running Cisco IOS Release 15.0(1)M3.

Workaround: There is no workaround.

- CSCtj32920

Symptoms: Packet drop seen while pinging from UUT to Pagent through VLAN.

Conditions: The symptom is observed on a router that is running Cisco IOS interim Release 15.1(3.1)T.

Workaround: There is no workaround.

- CSCtj34061

Symptoms: System reloads during a conference call that is established between an analog/FXS endpoint and SIP phones (SPA 50x/30x).

Conditions: The symptom is seen under the following conditions:

1. Analog phone calls SPA-1 phone.
2. Press flash on the analog phone and call SPA-2 phone.
3. After SPA-2 answers, press flash to conference all phones.

Workaround: There is no workaround.

- CSCtj35106

Symptoms: Spurious memory access seen:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x61CBC400z reading 0x70
%ALIGN-3-TRACE: -Traceback= 0x61CBC400z 0x631A1ABCz 0x63156BA0z 0x631A508Cz
0x631A5600z 0x62B75A10z 0xFFFFF95C0z 0xFFFFF95C0z
0x61CBC400:ipv6_enqueue(0x61cbc3dc)+0x24
0x631A1ABC:fw_dp_insp_send_rsts(0x631a00b8)+0x1a04
0x63156BA0:fw_dp_tcp_inactivity(0x631567ac)+0x3f4
0x631A508C:fw_dp_insp_handle_sis_idle_timeout(0x631a4c64)+0x428
0x631A5600:fw_dp_insp_handle_timer_event(0x631a554c)+0xb4
0x62B75A10:tw_notify(0x62b75944)+0xcc
```

Conditions: The symptom is observed with any self-generated IPv6 traffic.

Workaround: There is no workaround.

- CSCtj35148

Symptoms: On a Cisco 3945, configuration for more than 256 dialer interfaces is disallowed.

Conditions: The symptom is observed with more than 256 dialer interfaces configured.

Workaround: Configure dialer maps with rotary-groups (we do not know the scale numbers for this and whether it will support say, 512 maps per interface).

- CSCtj35792

Symptoms: The onboard GE on a Cisco 3900 (driver PQ3_TSEC) with “media-type sfp” goes to 1000/HD when it is connected by fiber to a gig port that is not doing autonegotiation.

Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation.

Workaround: Configure autonegotiation on the other side, if possible.

The Cisco 3945-E does not have this problem.

Further Problem Description: It is impossible to disable autonegotiation on the Cisco 3900 because of CSCth72105.

- CSCtj38234

Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

Workaround: There is no workaround.

- CSCtj38492

Symptoms: Hold resume fails when there is a redirected call from CUCM transit via CUBE.

Conditions: The symptom is observed with CUCM 7.1.

Workaround: There is no workaround.

- CSCtj38519

Symptoms: EIGRP pacing timer is large when there is a large number of peers on NBMA interfaces.

Conditions: The symptom is observed when EIGRP is configured with a large number of peers on a single NBMA interface.

Workaround: Ensure spokes are setup as stub and properly summarized.

- CSCtj39558

Symptoms: Sub-interface queue depth cannot be configured.

Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

Workaround: There is no workaround.

- CSCtj39777

Symptoms: A Cisco 2921 router crashes with IPSec and QoS.

Conditions: The symptom is observed on a Cisco 2921 router when QoS pre-classify is enabled.

Workaround: There is no workaround.

- CSCtj41867

Symptoms: A Cisco 2900 Integrated Service router that is running Cisco IOS Release 15.1(2)T exhibits increased memory utilization over time.

Conditions: The symptom is observed when a Cisco 2900 Integrated Services router that is running Cisco IOS Release 15.1(2)T is configured as a branch router that has an VPN WAN connection, Quality Of Service (QoS) classification configured ("qos pre-classify"), and WAAS Express enabled on a several interfaces with MLPPP enabled.

Workaround 1: Disable QoS classification on VPN tunnel interface.

Workaround 2: Disable WAAS Express on VPN tunnel interface.

Workaround 3: Reduce the number of serial interfaces down to one

Further Problem Description: The symptom is not observed when QoS classification is not configured or when MLPPP is not configured or when WAAS Express is not enabled.

- CSCtj44343

Symptoms: The output from commands executed using the **exec** Tcl command cannot be saved into variables. Instead, the output is redirected to the terminal.

Conditions: This occurs after running a Tcl script a number of times. For example, the issue has been seen after running a Tcl script four times. After the fourth time the output will not be saved in variables.

Workaround: There is no workaround.

- **CSCtj44520**
 Symptoms: System crashes with memory block corruption.
 Conditions: The symptom is observed when running traffic with QoS, crypto, tunneling, and MLPP features enabled.
 Workaround: Remove one of the features.
- **CSCtj46670**
 Symptoms: When a dialer interface has moved out from standby mode when the primary link is up, you cannot open LCP since you reply with an IPCP CONFREJ. Also dialer string is needed to be configured for PPPoX scenario, as per debug dialer events.
 Conditions: The symptom is observed when a dialer interface has moved out from standby mode.
 Workaround: Reload the router.
 Further Problem Description: When enabling dialer debugs the following error message is seen:
 Di1 DDR: Cannot place call, no dialer string set
- **CSCtj46843**
 Symptoms: Gateway detects the fax tone but does not initiate NSE packets towards the originating gateway.
 Conditions: The symptom is observed on a Cisco 3945 router that is running Cisco IOS Release 15.0(1)M3 and with DSP code: 26.3.7.
 Workaround: There is no workaround.
- **CSCtj47696**
 Symptoms: A Cisco 3845/3925 router will not process any in/outgoing ISDN calls once the network derived clock is configured (i.e.: “network-clock-participate wic 0”).
 Conditions: The symptom is observed on a Cisco 3800 or 3900 series router with NM-8CE1T1-PRI or HWIC-2CE1T1-PRI that is running Cisco IOS Release 15.1 (1)T or Release 12.4(24)T4 deriving the clock from the network.
 Workaround: Configure local clocking (“no network-clock-participate”) and reload.
 Further Problem Description: With “no network-clock-participate” configured, a call will succeed on ISDN layer but an analog call will fail due to lack of synchronization between the PVDM and the PRI.
- **CSCtj47829**
 Symptoms: A buffer leak is experienced with “traffic-export” configured.
 Conditions: The issue seen when you export traffic to an interface and to an NME-APPRE-502-K9. All conditions are not completely known yet.
 Workaround: Disable the traffic-export functionality, for example:
 Traffic export configs:


```

ip traffic-export profile axp-netscout
interface Integrated-Service-Engine1/0
bidirectional
mac-address 0080.8c00.0001

interface FastEthernet0/0.99
encapsulation dot1Q 99
ip address xxx.xxx.xxx.xxx 255.255.255.0
ip traffic-export apply axp-netscout
    
```

Remove the configs:

```
interface fa0/0.99
no ip traffic-export apply axp-net scout
no ip traffic-export profile axp-net scout
```

- CSCtj48242

Symptoms: A memory leak is seen in the processor memory. The **show mem debug leaks summary** command shows that “Presence Process” and “mem_mgr: mem_mgr_malloc_buf” is leaking.

Conditions: The conditions are not fully known yet. It looks like the issue is related to SIP traffic.

Workaround: There is no workaround.

- CSCtj48629

Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtj48913

Symptoms: Track does not recognize when an HTTP IP SLA probe’s status changes to OK.

Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

Workaround: There is no workaround.

- CSCtj49133

Symptoms: After attaching a policy-map to a sub-interface, the policy-map is then renamed and then the sub-interface is deleted. The policy-map definition can not be deleted and still shows up in the running configuration.

Conditions: The symptoms are observed with the following steps:

1. Attach a policy to a sub-interface.
2. Rename the policy-map.
3. Remove the sub-interface.
4. Removing the definition of policy-map will not succeed.

Workaround: Remove the service policy from sub-interface before removing the sub-interface.

- CSCtj49957

Symptoms: Multicast source NAT translation does not work correctly with simultaneous replication to both inside and outside interfaces.

Conditions: The symptom is observed when replicating the multicast feed from a NAT inside interface to both a NAT inside and outside interface simultaneously. The intended result: translated packets to the outside interface being translated but not packets to the inside interface.

Workaround: There is no workaround.

- CSCtj52795

Symptoms: Crash is seen when unconfiguring the service policy under the tunnel interface.

Conditions: The symptom is observed when the tunnel interface comprises NAT and multicast configurations.

Workaround: There is no workaround.

- CSCtj53363

Symptoms: Router hangs and console does not respond indefinitely.

Conditions: The symptom is observed with the following conditions:

- AIM-VPN in ISR + ZBFW; or
- A Cisco 2811/2821 Onboard VPN + ZBFW.
- Once traffic starts, router hangs within minutes.

Workaround 1: If running a Cisco 2811/2821, use sw crypto + ZBFW.

Workaround 2: If running with a Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj53407

Symptoms: When WAN interfaces of 860, 880, and 890 are configured for fixed speed/duplex settings (100/full, 100/half, 10/full, 10/half), the link goes down. Autonegotiation works fine.

Conditions: Both the ends of the link should be configured for fixed speed/duplex settings.

Workaround: There is no workaround.

- CSCtj54666

Symptoms: IP jitter statistics table is corrupted when rttMonApplTimeOfLastSet rolls over the 32 big mark.

Conditions: The symptom is observed with the IP jitter statistics table.

Workaround: There is no workaround.

- CSCtj55834

Symptoms: Input drops seen when “queue-limits” are applied.

Conditions: The symptom is observed when using traffic policing and queue limits in a child policy-map. This occurs when the configured queue-limit is much higher than the default of 64 and may be due to buffer starvation.

Workaround: Use a lower value or the default of 64.

- CSCtj56519

Symptoms: Multicast over VMI in NBMA-mode fails with IGMPv3.

Conditions: This issue is seen in routers loaded with Cisco IOS interim Release 15.1(2.19)T0.1.

Workaround: There is no workaround.

- CSCtj58458

Symptoms: A Cisco IAD887 fails to respond because of an IO buffer leak.

Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T.

Workaround: Reload the router.

- CSCtj58489

Symptoms: Path confirmation failure for DO-EO with VCC and HD configurations.

Conditions: The symptom is observed with a DO-EO with HD Transcoding and VCC configured. The following cases are failing because of this issue:

```
BC_DO-EO_FA_VCC_SS_ReINV_HD
BC_DO-EO_FT_VCC_SS_ReINV_HD
BC_DO-EO_FA_VCC_EQ_ReINV_HD
BC_DO-EO_FT_VCC_EQ_ReINV_HD
```

Workaround: There is no workaround.

- CSCtj59117

Symptoms: The following error message is seen and the router freezes and crashes:

```
%SYS-2-BADSHARE: Bad refcount in retparticle
```

A reload is required to recover.

Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.

Workaround: Remove CEF.

- CSCtj61284

Symptoms: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

Workaround: There is no workaround.

- CSCtj61657

Symptoms: IO memory leak is seen followed by TCP no buffer logs:

```
%SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0XXXXXXXXX, alignment
xxx Pool: I/O Free: xxxx Cause: Not enough free memory Alternate Pool: None Free: 0
Cause: No Alternate pool -Process= "Pool Manager"
%TCP-6-NOBUFF: TTY0, no buffer available -Process= "SCCP Application", ipl= 0, pid=
XXX
```

Conditions: The symptom is observed in the presence of VOIP phones using multicast applications with the **session protocol multicast** dial-peer configuration command.

Workaround: There is no workaround.

- CSCtj63307

Symptoms: GRE fragments get dropped.

Conditions: The symptom is observed with GRE fragments. The parent bug is CSCsv68549.

Workaround: There is no workaround.

- CSCtj63943

Symptoms: There is a router crash on applying **tunnel mode ipsec ipv4** under a tunnel interface.

Conditions: The symptom is observed when the tunnel interface is up while configuring the command.

Workaround: There is no workaround.

- CSCtj66235

Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

```
%SYS-6-STACKLOW: Stack for process voice file acct dump running low, 0/6000
```

Conditions: The crash suggests that the issue is just one of inefficient stack usage.

Workaround: There is no workaround.

- CSCtj66392

Symptoms: Tunnel interface does not go up on standby router and IKE and IPSec SAs are not synchronized to the standby router. Even if tunnel protection is configured, crypto socket is not opened.

Conditions: This symptom is observed when IPSec stateful failover for tunnel protection is configured.

Workaround: Use Cisco IOS Release 12.4(11)T4.

- CSCtj67047

Symptoms: While testing “PPP Cell Phone Negotiation” (MLP CEF switching), you may be unable to retrieve the total count of packets that are CEF-switched.

Conditions: This issue is seen in a router that is loaded with Cisco IOS interim Release 15.0(1)M3.11.

Workaround: There is no workaround.

- CSCtj67845

Symptoms: A Cisco 2951 router crashes on power up.

Conditions: The symptom is observed on a Cisco 2951 router when an HWIC-ADSL and EHWIC-VA-DSL are plugged in together.

Workaround: There is no workaround.

- CSCtj69577

Symptoms: When congestion occurs on a QoS-enabled output interface, output rate significantly decreases.

Conditions: The symptoms are observed under the following conditions:

1. 3945E outbound interface is connected to 100M link.
2. QoS (LLQ/Fair Queue) is configured on 3945E outbound interface.
3. Congestion occurs on outbound interface.

Workaround: Reload the router.

Further Problem Description: This issue is resolved after a reload but the shutdown/no shutdown commands can cause the same issue.

- CSCtj72592

Symptoms: Crypto engine drops packets.

Conditions: The symptom is observed on a Cisco 3900 that is running Cisco IOS Release 15.1(2)T with an output service-policy.

Workaround: Remove QoS.

- CSCtj76297

Symptoms: Router hangs with interoperability of VM and crypto configurations.

Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

Workaround: Disable AIM and use onboard CE.

- CSCtj77285

Symptoms: Router CPU becomes high tending towards 80%+ from normal operating conditions. The command **show mem | inc FNF OCE** will show multiple rows rather than just a couple of rows.

Conditions: The symptom is observed with voice calls and VOIP in use. It is seen when Flexible NetFlow is configured.

Workaround: Switch off Flexible NetFlow (although that leaves memory consumption in place and CPU higher than normal) or reboot the router.

- CSCtj77477

Symptoms: High LLQ delay.

Conditions: The symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E. There is high delay in priority queue when using CBWFQ/LLQ. For example:

```
EFM rate 2304 kbps
888E Average delay: 42ms
888E Max delay: 63ms
HWIC-4SHDSL-E Average delay: 216ms
HWIC-4SHDSL-E Max delay: 361ms
```

Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface. For example:

```
EFM rate 2304 kbps

policy-map CHILD
  class voice
    priority percent 25
  class business
    bandwidth percent 50
policy-map PARENT
  class class-default
    shape average 2100000 8400 0
  service-policy CHILD
```

- CSCtj77819

Symptoms: When dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration), then it is not effective. It is not resetting the idle timeout when outgoing interesting traffic is seen.

Conditions: The symptom is observed when dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration).

Workaround: Reconfigure “dialer idle-timeout” with any value (even default of 120 secs).

- CSCtj78107

Symptoms: A Cisco 87X series router may show this message:

```
%OCE-3-OCE_FWD_STATE_HANDLE with SW Crypto
```

When this message occurs, the router stops passing any traffic and has to be rebooted.

Conditions: The symptom is observed when the router is running the software encryption engine. Every couple of days the following message appears on the console:

```
Limit of oce forward state handle allocation reached; maximum allowable number is
50000
```

Workaround: Disable CEF (causes CPU spikes).

- CSCtj78210

Symptoms: One-way audio. Moves from one port to another when the router is rebooted.

Conditions: The symptom is observed when using multiple “session protocol multicast”, “connection trunk” configurations for LMR, E&M Immediate, and/or other multicast applications, such as the conditions where this was first detected, in a Radio over IP solution. Only affects PVDM3.

Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

For example, configure:

```
voice-card 0 (1... 2... etc...)
dspfarm
dsp service dspfarm
```

```

dspfarm profile x conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x2 conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x3 conf
max sessions xx << use maximum (if allowed)
max partic << use the maximum (if allowed)
associate app sccp
no shutdown

```

```

dspfarm profile x conf
shutdown
no dspfarm profile x conf

```

The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- CSCtj78407

Symptoms: Router crashes.

Conditions: The symptom is observed when attempting to launch CP Express.

Workaround: A reload of the router fixes this issue temporarily.

- CSCtj78836

Symptoms: A Cisco 3900 series router may undergo a software-forced reload.

Conditions: This condition is observed with Cisco IOS interim Release 15.1 (2.19)T0.4, and only when Video Monitoring (VM) policy is configured.

Workaround: Do not configure a VM policy.

- CSCtj79368

Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

Conditions: The symptom is observed when removing RSA keys.

Workaround: Stay on the same RSA keys.

- CSCtj79476

Symptoms: Traffic loss and VLAN related errors seen when the traffic is sent for a prolonged duration on an HWIC-4ESW.

Conditions: The symptom is observed when traffic is sent for a prolonged duration (>12hrs) on an HWIC-4ESW.

Workaround: There is no workaround.

- CSCtj79480

Symptoms: High CPU usage due to time_it (in interrupts).

Conditions: The conditions are undetermined at this time.

Workaround: Reload the router and the CPU goes down for certain time.

- CSCtj79761

Symptoms: All bearer channels in T1 PRI are not engaged.

Conditions: The symptom is observed when dialer is configured and more than T1 line rate traffic is sent.

Workaround: There is no workaround.

- CSCtj79765

Symptoms: Attributes downloaded from AAA server are not applied to UUT.

Conditions: The symptom is observed with attributes downloaded from AAA server.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(3)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsb14936

Symptoms: SNMPv3 gets/sets fail following a PRE switchover. Attempts increment `usmStatsWrongDigests.0`.

Conditions: This symptom is observed in configurations with RPR+ and that use SNMPv3, where the `snmp EngineID` value is the default value.

Workaround: The workaround for this symptom is to specify a value for the `snmp EngineID` via the global configuration cli “`snmp-server engineID local [octet string]`,” where `octet string` is the desired `engineID` value.

Further Problem Description: Once the device is upgraded to an image that has this fix, and if the device does not have “`snmp-server engineID local [octet string]`” configured, then all the existing v3 `authNoPriv/authPriv` users will not work. The v3 `authNoPriv/authPriv` users will have to be reconfigured.

- CSCsk55161

Symptoms: Cisco IOS software crashes when enabling multicast feature of scaled-up config.

Conditions: This symptom is observed under the following conditions:

- More than 4000 VLANs are configured on a Port Channel.
- All VLANs have a V6 configuration, and multicast is enabled on each of them at once.

Workaround: There is no workaround.

- CSCsk82537

Symptoms: About once every 1 or 2 minutes, the value of the delta time found in the responding router in an IP SLA setup is 1 second behind the value it should have. This is causing false timeout as the RTT is then considered as being around 24 hours. The following output illustrates this problem:

```
IP SLAs(100) jitter operation: Timed out arrival (rtt=86399012)
For 3 consecutive probes:
```

ST: 75656998, RT: 75657005, DT: 0, CT: 75657014 => correct ST: 75658006, RT: 75658009, DT: 0, CT: 75657018 => should be 75658018 ST: 75659006, RT: 75659009, DT: 0, CT: 75658018 => should be 75659018 ST: 75659998, RT: 75660005, DT: 0, CT: 75660014 => correct

Conditions: This has been seen on a Cisco 1812 running Cisco IOS Release 12.4(6)T7.

Workaround: There is no workaround.

- CSCso02147

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCso20810

Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. This occurs when multicast subsequently flows out a crypto-enabled interface.

Conditions: This symptom will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCsu95339

Symptoms: Output from the **show idmgr session** command displays a corrupted service name.

Conditions: Enter the **show idmgr session command**.

Workaround: There is no workaround.

- CSCsw38009

Symptoms: Packet drops are seen on an ATM interface when it is used as a tunnel source.

Conditions: This symptom is observed as soon as Per SA QoS is configured on the tunnel interface.

Workaround: This symptom is not seen on Ethernet.

- CSCsz79652

Symptoms: A memory leak may be seen in Dead memory.

Conditions: This symptom is observed in Cisco IOS Release 12.2(50)SE and Release 12.2(50)SE1. Cisco IOS Release 12.2(44)SE is not affected. The symptom occurs when using Cisco Network Assistant to poll the device. The **ip http server** command or **ip http secure- server** command must be enabled for the leak to occur.

Workaround: Disable the http server or stop CNA from polling the device.

- CSCta53372

Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

Workaround: Reset the RRI session.

- CSCta79941

Symptoms: A virtual interface is not created when invoked using the **ip unnumbered type number** command.

Conditions: This symptom is observed under a PPP interface when the virtual interface has been previously deleted.

Workaround: Recreate the virtual interface manually using the **interface** command.

- CSCta91928

Symptoms: A Cisco 881GW with a 3G modem may crash when the modem is reset or power-cycled.

Conditions: This symptom is observed on a Cisco 501 or 880 with a 3G modem when “test cellular 0 modem-power-cycle” or “test cellular 0 modem-reset” is entered.

Workaround: There is no workaround.

- CSCtb55576

Symptoms: When an HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

Workaround: There is no workaround.

- CSCtb57180

Symptoms: A router may crash with a software-forced crash.

Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

The following example permits access to VTYS from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255 Router(config)#
access-list 1 permit host 172.16.1.2 Router(config)# line vty 0 4 Router(config-line)#
access-class 1 in
```

For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x> Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.
3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.
4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.
5. Avoid issuing the **show users** command repetitively in a short period of time.

Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- CSCtb69063

Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:

```
config# username <name of 64 characters> priv <0-15> password 0 <password>
```

Conditions: The symptom is observed if the user name is exactly 64 characters.

Workaround: Configure a user name of 63 characters or less.

Further Problem Description: When some configurations are added, modified, or deleted the **show configuration id detail** command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the “changed by user” field prints unwanted characters.

- CSCtb89424

Symptoms: In rare instances, a Cisco router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

```
hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC  
= 0x424ECCE4
```

Conditions: This symptom is observed while using IP SLA.

Workaround: There is no workaround.

- CSCtc33679

Symptoms: Routes are not being controlled properly when PIRO is used.

Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

Workaround: There is no workaround.

- CSCtc52299

Symptoms: UDP packets broadcast with destination port 53 for 10 minutes bring the CPU to 100% and cause a router crash if the dns server is removed.

Conditions: This symptom is observed with UDP broadcast at port 53, which causes the port to remain open and the CPU hog to occur in 5-10 minutes. The router CPU reaches 100% capacity and does not come down even after the broadcast traffic is stopped.

Workaround: There is no workaround.

- CSCtc55897

Symptoms: R2 will not advertise the routes.

Conditions: The symptom is observed under the following conditions:

1. R2 has two IBDG neighbors in the same update-group: one neighbor with 4BAS and the other with 2BAS capability.
2. The locally originated routes or routes without any AS_PATH will not be advertised to this kind of group.

Workaround: Try to make the 2BAS and 4BAS neighbors fall into different update-groups by configuring dummy route-maps.

- CSCtc58917

Symptoms: Dialer idle timeout is not being reset with interesting traffic.

Conditions: This symptom is observed when MPPC compression is turned on.

Workaround: There is no workaround.

Further Problem Description: A call is made from Windows XX client dial-up networking to the NAS. After the call is established and interesting traffic is sent every 30 seconds for 180 seconds, idle timeout is not being reset.

- CSCtc71408

Symptoms: Fax transmission fails when CUBE is in the middle.

Conditions: The symptom is observed when either one of the dial-peers on OGW/TGW/CUBE is configured for fax protocol T38 version 0.

Workaround: Configure version 3 on all dial-peers.

- CSCtc78200

Symptoms: A Cisco router may crash in the parse_configure_idb_extd_args routine.

Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

Workaround: As PPP session is being established on the LNS, IOS will momentarily use one of the available VTYs from the router. After initial configuration is done, it is immediately released to the system pool.

If all VTY connections are in use, then we will see an RP crash if a new PPP session is being established and there are no free VTYs in the system.

To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect thereby using multiple VTY connections at the same time, it is recommended to reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:

```
ip access-list extended VTY_ACL deny ip any any ! line vty 5 9 access-class VTY_ACL
in exec-timeout 1 0 login authentication local1
```

Alternate Workaround: Do not configure “interface range” cli using ios_config from tcsh mode. When in tcsh mode, use normal “interface cli” in a “for loop.”

- CSCtd30544

Symptoms: Netflow is showing Null in the destination interface even though packets are not getting dropped or blocked.

Conditions: This symptom is seen when connected to the LNS via VPDN and browsing HTTP. Intermittently Null output is seen as the destination interface as the packet being punted between different CEF switching paths due to **ip tcp adjust-mss** *value* configuration that is applied on the destination interface.

Workaround: Remove **ip tcp adjust-mss** *value* from the destination interface.

- CSCtd31465

Symptoms: An H323 to SIP CUBE may get stuck in a race condition if a reINVITE with delayed media is quickly followed by a reINVITE with early media while still renegotiating the H323 side of the call for the delayed media INVITE. This may lead to one-way or no-way audio.

Conditions: This symptom was observed with the following topology: IP phone---CUCM---H.323 Fast Start---CUBE---SIP---3rd-party SIP server--- CallCenter

Calls flow from the IP phone to the CallCenter hanging off a 3rd-party device. The 3rd-party device re-INVITES, rapidly, as calls traverse through its menu/IVR system.

Workaround: There is no workaround.

- CSCtd39579

Symptoms: A router crashes when we try to remove service-policy/waas from an interface.

Conditions: Traffic should be hitting the interface, CPU utilization should be high, and NAT should be applied on the interface as well.

Workaround:

1. Remove NAT from the interface
2. Remove the service policy
3. Re-apply NAT.

- CSCtd54301

Symptoms: A Cisco router gets stuck in syntax-conf-ssh-pubkey-data mode, and you are not able to exit from syntax-conf-ssh-pubkey-data mode.

Conditions: This symptom is observed on a Cisco 7200 router loaded with a Cisco IOS 15.1(0.17)T image.

Workaround: There is no workaround.

- CSCtd59027

Symptoms: A Cisco device crashes due to a bus error.

Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCtd62885

Symptoms: IKE renegotiation might fail for minutes while one peer displays:

```
%CRYPTO-6-IKMP_NOT_ENCRYPTED:
```

IKE packet from <ip> was not encrypted and it should have been

Conditions: The symptom is observed when certificates are used. The signature verification might fail after MM5 or MM6 messages are exchanged preventing the tunnel establishment. The issue seems to affect Cisco IOS Release 12.4(20) T3 and Release 12.4(24)T2. It affects only Cisco 7200 series routers with VSA modules.

Workaround: Use pre-shared keys.

- CSCte07666

Symptoms: A Cisco router may crash when the TCL script without_completion.tcl is run.

Conditions: This symptom is observed when running the TCL script without_completion.tcl as the script tries to fill in the _cerr_name field with an array that is not sufficiently populated.

Workaround: There is no workaround.
- CSCte17560

Symptom: Offered rate in QoS class shows unusually high values.

Conditions: The symptom is observed when service-policy is applied on a multilink interface.

Workaround: There is no workaround.
- CSCte18124

Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with "atm vc-per-vp 1024".

Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when "atm vc-per-vp 1024" is configured.

Workaround: Create ATM PVC without "atm vc-per-vp 1024".
- CSCte20187

Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (1)
```

The label advertised may be different but it is always a reserved label (0- 15).

Additionally, the local PE will see "No Label" as the Outgoing Label" in the MPLS forwarding table.

Conditions: This symptom is observed when bgp next-hop is configured under an interface.

Workaround: There is no workaround.
- CSCte27828

Symptoms: Call forward does not work.

Conditions: Topology: call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider.

IP addresses: CUCM10.10.10.3 Cube SUD10.10.10.2 CUBE North192.168.101.10 SBC 192.168.100.5

"Call forward no answer" scenario does not work, but not systematically: sometimes it works, sometimes not.

When the "call forward no answer" fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC doesn't answer due to this.

Workaround: There is no workaround.
- CSCte61495

Symptoms: The following messages are seen with tracebacks:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process = Exec. %SYS-2-INTSCHED: 'suspend' at level 3 -Process= "Exec", ipl= 3, pid= 128,
```

Conditions: The symptom is observed when a large ACL is configured for the service-policy. This happens only under ATM subinterfaces.

Workaround: Use small sized ACLs for the service-policy.

- CSCte82226

Symptoms: While changing the MTU on a Port-channel, you may see the following traceback:

`SYS-SP-2-NOBLOCK error`

Conditions: This symptom is observed when changing the MTU on a Port-channel.

Workaround: There is no workaround.

- CSCte85961

Symptoms: The router crashes while doing a **shut** command followed by the **no shut** command to the main interface.

Conditions: The issue is seen with scale configuration and giving the **shut** command followed by the **no shut** command in the main ATM interface.

Workaround: There is no workaround.

- CSCte86038

Symptoms: High CPU utilization for ATM OAM timer process.

Conditions: The symptom is observed with a scaled L2 VC configuration.

Workaround: Increase the AIS RDI timeout with higher number of up and down retries.

- CSCte89130

Symptoms: Router experiences a memory leak.

Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).

Workaround: There is no workaround.

- CSCte91259

Symptoms: A Cisco router may unexpectedly reload due to a bus error after displaying an “%IDMGR-3-INVALID_ID” error.

Conditions: The crash will be seen only if the router is using DHCP Client Dynamic DNS update.

Workaround: There is no workaround.

- CSCte92581

Symptoms: A VRF becomes stuck during deletion in a rear condition (not something that is seen every time).

Conditions: This symptom is observed when the **no ip vrf** command is entered.

Workaround: There is no workaround.

Further Problem Description: The stuck VRF cannot be reused.

- CSCte93792

Symptoms: Virtual access bound to an ATM interface does not come up.

Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.

Workaround: There is no workaround.

- CSCte94301

Symptoms: IPv6 PBR is not applied to locally-originated ping packets.

Conditions: This symptom occurs when IPv6 PBR is configured for application to locally-originated ping packets.

Workaround: There is no workaround.

- CSCte95301

Symptoms: Memory leak in proxy authentication scenario, when authentication fails.

Conditions: The symptom is observed when HTTP proxy authentication is used.

Workaround: There is no workaround.

- CSCtf06436

Symptoms: Continuous high CPU usage.

Conditions: The symptom occurs after the formation of a recursion loop in the FIB, when the prefixes in the loop are labeled.

Workaround: There is no workaround.

- CSCtf25293

Symptoms: SSH connection to a SSH server aborts abruptly after making the connection, while using public key-based authentication.

Conditions: Authentication method used must be public key.

Workaround: Use kbd-interactive or password-based authentication.

- CSCtf35006

Symptoms: If there are two jobs in an SNMP job queue and if you try to destroy the jobs, the console hangs.

Conditions: The symptom is observed if you prepare multiple license action entries and then let them execute immediately.

Workaround: There is no workaround.

- CSCtf40025

Symptoms: "IP SLAs XOS Event Processor" process hangs and input queue of an interface is stuck.

Conditions: This symptom observed in Cisco IOS Release 15.1T when IP SLA UDP jitter operations are restarted via SNMP.

Workaround: There is no workaround, except for a router reload.

- CSCtf47929

Symptoms: Tracebacks are seen on a Cisco router when creating a udp-jitter operation with request-data size of more than 17000 bytes (super jumbo packet).

Conditions: This symptom is observed with a large request-data size.

Workaround: Use a request-data size value less than 17000.

- CSCtf48094

Symptoms: UUT crashes for FTP traffic with debugs enabled for IPv6 inspection.

Conditions: The symptom is observed only with Legacy Firewall for IPv6 inspection.

Workaround: There is no workaround.

- CSCtf48179

Symptoms: When using an authentication header only (no encryption over the tunnel), a percentage of the outgoing traffic is dropped by the receiver due to incorrect IP header checksums. The percentage dropped depends on the traffic that is flowing over the tunnel.

Conditions: This problem occurs only when the traffic mix over the tunnel includes both packets with the DF bit set and packets with the DF bit clear. When the DF bit setting differs between two subsequent packets, the second packet is sent with an incorrect IP header checksum.

Workaround: There is no workaround.

- CSCtf70365

Symptoms: When “config ED” is used for EEM with some special configurations (like virtual-template commands), it can trigger error messages.

Conditions: The symptom is observed only when certain commands are configured.

Workaround: Use “syslog ED”.

- CSCtf77047

Symptoms: Ping ATM subinterface peer IP address has packet loss from Cisco 7206.

Conditions: This symptom occurs with the following:

1. NPE-G2+PA-MC-STM-1SMI+PA-A6-OC3SML
2. Enable EIGRP on ATM subinterface

Workaround: There is no workaround.

- CSCtf78196

Symptoms: Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

Conditions: The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface.

Workaround: Statically configure “ipv6 mtu <mtu>” on tunnel interfaces.

- CSCtf79264

Symptoms: A Cisco route processor (RP) loses part of its odr-route for the spoke network. With a busy network, and with more than 1000 spokes, the second RP can have the same symptom.

Conditions: This symptom is observed with a default odr timer.

Workaround: Modifying the odr timer can help, but will not solve the problem.

- CSCtf84393

Symptoms: A Cisco gateway is unable to place outbound calls from the BRI port when the MGCP gateway is in SRST mode. The call disconnects with cause value = 63 (service/option not available).

Conditions: This symptom is observed in Cisco IOS Release 12.4(20)T4, Release 12.4(24)T2, and Release 15.0(1).

Workaround: There is no workaround.

- CSCtf98087

Symptoms: A Cisco router reloads at sipSPIUpdSrtpSession.

Conditions: This symptom is observed after completion of the basic call with a hold/resume scenario with IPv6 mode.

Workaround: There is no workaround.

- CSCtg08496

Symptoms: After merge, keyserver deletes all GMs so the rekey fails to be sent (DB is empty) and all the GMs need to re-register.

Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtg14446

Symptoms: Packets are dropped in excess of the configured rate for hierarchical policies, with shaper in the parent policy.

Conditions: The symptom is observed only with HQoS policies (flat policies are not affected).

Workaround: There is no workaround.

- CSCtg19546

Symptoms: MPLS forwarding of labeled frames across a tunnel may fail. This symptom arises when an incorrect TAG adjacency is created for the tunnel.

Conditions: This symptom is observed when adding or removing crypto and a tunnel protection configuration from a tunnel interface also configured with MPLS. When this symptom occurs, an incorrect or missing IPsec post encaps feature is observed under the TAG adjacency for the tunnel.

Workaround: Removing the crypto and/or removing and reconfiguring mpls ip from the tunnel can recover connectivity.

Alternate Workaround: VTI cannot be combined with MPLS label switching, since IPsec can only encapsulate IP packets, not MPLS packets. This is due to design. In GRE mode, however, this is possible, so use a GRE tunnel with IPsec tunnel protection along with MPLS label switching. Be sure to remove and reapply the “tunnel protection ipsec profile” configuration so that IPsec features will be properly applied to the IP-and MPLS-switching feature paths.

- CSCtg25798

Symptoms: The issue is associated with the two labels imposition for the next-hop address. If there is no label bind for the destination prefix and in order to reach next-hop address the router imposes two labels, only one label is imposed for the final prefix.

Conditions: The symptom occurs when all of the following conditions are met:

1. The prefix does not have a label bind (BGP prefixes for example).
2. There is a static route for the next-hop address pointing to the tunnel only.
3. The router imposes two labels for the next-hop address.

Workaround: There are three potential workarounds:

1. Explicit next hop avoiding recursive research: “ip route 192.168.4.4 255.255.255.255 Tu1 192.168.4.4” (i.e.: breaking rule 2).
2. Use “neighbor 192.168.1.1 send-label” on both PEs (i.e.: breaking rule 1).
3. Use “mpls traffic-eng signaling interpret explicit-null verbatim” on P (i.e.: breaking rule 3).

Further Problem Description: In the following example 192.168.200.200 is the final destination. There is no label bind for this prefix and it is recursive to 192.168.100.100:

```
PE1#sh mp ld bin 192.168.200.200 32 lib entry: 192.168.200.200/32, rev 35 local
binding: label: 31
```

```
PE1#sh ip route 192.168.200.200 Routing entry for 192.168.200.200/32 Known via
“static”, distance 1, metric 0 Routing Descriptor Blocks: * 192.168.100.100 Route
metric is 0, traffic share count is 1
```

The next-hop 192.168.100.100 has a static route pointing to the tunnel and is double tagged:

```
PE1#sh ip route 192.168.100.100 Routing entry for 192.168.100.100/32 Known via
"static", distance 1, metric 0 (connected) Routing Descriptor Blocks: * directly
connected, via Tunnel10 Route metric is 0, traffic share count is 1
PE1#sh ip cef 192.168.100.100 192.168.100.100/32 attached to Tunnel10 label 26
PE1#sh mp ld bin 192.168.100.100 32 lib entry: 192.168.100.100/32, rev 30 local
binding: label: 29 remote binding: lsr: 192.168.2.2:0, label: 26 remote binding: lsr:
192.168.4.4:0, label: 26 <<<< tunnel head-end
```

So the traffic to 192.168.200.200 should also be double tagged as shown below:

```
PE1#sh ip cef 192.168.200.200 192.168.200.200/32 nexthop 192.168.100.100 Tunnel10
label 26
```

However traffic is leaving the router only with the tunnel label:

```
PE1#trace 192.168.200.200 Type escape sequence to abort. Tracing the route to
192.168.200.200 1 192.168.12.2 [MPLS: Label 20 Exp 0] 4 msec 0 msec 0 msec 2
192.168.23.3 [MPLS: Label 23 Exp 0] 4 msec 0 msec 0 msec 3 192.168.34.4 4 msec 0 msec
0 msec 4 192.168.48.8 4 msec * 4 msec
```

- CSCtg30795

Symptoms: Calls are not torn down since SIP INFO with Qsig disconnect tunneled are not honored by the SIP gateway.

Conditions: This symptom is observed when disconnect is built and sent by Call manager over a Qsig-enabled SIP trunk to the SIP gateway (GW).

CUCM1---SIP-QSIG----SIP GW-----T1 QSIG-----MGCPGW-----CUCM2

In the above setup, when CUCM1 initiates disconnect, it sends out INFO tunneled with Qsig disconnect to the SIP GW in order to achieve 3-way disconnect.

Workaround: There is no workaround.

Further Problem Description: The gateway should send a Qsig Disconnect over the T1 link; since that is not happening, the call is not torn down.

- CSCtg31434

Symptoms: A Cisco router crashes due to an unexpected exception to the CPU.

Conditions: This symptom occurs when the **privilege interface level 10 ppp authentication** command is entered. This symptom is observed in Cisco IOS Release 12.2(31)SB through Release 12.2(31)SB18, and in Cisco IOS Release 12.2(33)SB and Release 12.2(34)SB.

Workaround: There is no workaround.

- CSCtg32567

Symptoms: IPv6 global addresses are not installed on a DHCP PD client interface.

Conditions: This symptom is observed when a DHCP client is configured for prefix delegation as well as defined to get an IPv6 address through the prefix delegation. The prefix is obtained from the DHCP server as expected, but the global address is not assigned to the client interface.

Workaround: There is no workaround.

- CSCtg35257

Symptoms: The message "previous instance of CNS Event Agent still executing" is seen even if a CNS event is not configured.

Conditions: The symptom is observed if the **cns event <IP> encrypt** command is enabled and disabled.

Workaround: There is no workaround.

- CSCtg35298
Symptoms: Traffic drops are seen between two PEs after re-optimization.
Conditions: The symptom is observed with 16k VPLS VC, 4k scalable EoMPLS, 1K software EoMPLS, 600 primary tunnels to nPE1 and one tunnel to nPE2 from nPE3.
Workaround: There is no workaround.
- CSCtg41733
Symptoms: Certain crafted packets may cause a memory leak in the device in very rare circumstances.
Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.
Workaround: Disable SIP if it is not needed.
- CSCtg42279
Symptoms: A Cisco label switch router (LSR) crashes when an MPLS traceroute is issued.
Conditions: This symptom is observed when executing MPLS traceroute over a IPsec-protected GRE tunnel.
Workaround: There is no workaround.
- CSCtg44108
Symptoms: Bus error crashes occur frequently.
Conditions: This symptom is observed on a Cisco 3945e Integrated Services Router (ISR) running Cisco IOS Release 15.1(1)T. IPsec is configured on a GRE multipoint tunnel interface.
Workaround: There is no workaround.
- CSCtg47129
Symptoms: A memory leak is seen when NAT is configured.
Conditions: This symptom is observed when NAT is configured.
Workaround: There is no workaround.
- CSCtg49109
Symptom: After a switchover, some of the modules go to MajFail state.
Conditions: This issue is observed when high traffic is triggered, a lot of packets are dropped by the platform, and numerous IPC messages time out.
Workaround: There is no workaround.
Further Problem Description: Due to some unexpected events, one of the IPCs boolean “IPC message blocked” is failing to get set (that is, failing to get unblocked), which is in turn blocking the ICC process from processing further messages. This results in the failure.
- CSCtg50024
Symptoms: A router experiences crashes due to TLB (load or instruction fetch) exception.
Conditions: This problem is observed on a Cisco 7206VXR router with Cisco IOS Release 12.4(24)T2.
Workaround: There is no workaround.
- CSCtg52885
Symptoms: The HSRP state on dot1q sub-interfaces remain in INIT state.
Conditions: This symptom is observed after a physical link flap on a trunk port.

Workaround: Perform a shut/noshut on the interface.

- CSCtg53953

Symptoms: A standby router reloads due to a parser sync issue when applying certain neighbor commands (**neighbor** *<ip-address>* **disable-connected-check**, **neighbor** *<ip-address>* **peer-group pgrp**, and others).

Conditions: This symptom applies only to situations where *<ip-address>* is the IP address of a peer that has a dynamically created session (a neighborhood that is the result of the “bgp listen range...” feature).

Workaround: There is no workaround. Such a configuration should not be applied in the first place.

- CSCtg56013

Symptoms: Router crashes when initiating ping through the modem after router bootup.

Conditions: The symptom is observed when the modem fails to enumerate at bootup.

Workaround: There is no workaround.

- CSCtg58786

Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

Workaround: There is no workaround.

- CSCtg59158

Symptoms: A Cisco router console is flooded with the following error messages:

```
crypto_engine_ps_vec: DF_BIT_STATUS_OK Check failed crypto_engine_ps_vec:
DF_BIT_STATUS_OK Check failed
```

Conditions: This symptom is observed when new SAs are installed during rekeys or after clearing existing SAs. This symptom is observed when GETVPN (crypto map) is configured along with WAAS.

Workaround: Cryptomaps are not supported in the current phase of WAAS- Express. Please use VTI or unconfigure WAAS-Express.

- CSCtg59328

Symptoms: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

Conditions: This symptom is observed when the following tasks are completed:

- Bring up a PPPoE session and ensure that it is synced to standby.
- From the PPPoE client run the commands **no ip address** followed by **ip address negotiated** under the Virtual- template interface.
- As part of the **no ip address** command, the session would first go down on both active and standby. The **ip address negotiated** command would then trigger IPCP re-negotiation and the session would come up on active. On standby, the session remains down and the new IP address is not synced.

Workaround: There is no workaround.

- CSCtg59956

Symptoms: Active supervisor crashes when doing an SSO switchover.

Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

Workaround: There is no workaround.

- CSCtg60201

Symptoms: Unconfiguring the **maximum-path** command does not trigger a backup path calculation.

Conditions: This symptom is observed if additional-path install is configured along with the **maximum-path** command.

Workaround: Reconfigure “bgp additional-path install.”

- CSCtg60302

Symptoms: CPP ucode crashes after shutting down mpls-te tunnel interfaces.

ixia -----PE1 -----PE2 -----ixia

This is a 6PE topology with an MPLS TE tunnel between PE1 and PE2 and traffic passing through the TE tunnel. When the TE is shut down, the CPP crashes.

Conditions: This symptom is observed when the traffic rate is about 500 packets per second.

Workaround: There is no workaround.

- CSCtg68012

Symptoms: The following logs are created by the Cisco 6509 switch:

```
Apr 29 10:21:17.335 BST: %SCHED-3-THRASHING: Process thrashing on watched message
event. -Process= "RTTYS Process", ipl= 5, pid= 78 -Traceback= 410545B0 41054694
418628A8 Apr 29 10:22:57.379 BST: %SCHED-3-THRASHING: Process thrashing on watched
message event. -Process= "RTTYS Process", ipl= 5, pid= 78 -Traceback= 410545B0
41054694 418628A8 Apr 29 10:24:37.427 BST: %SCHED-3-THRASHING: Process thrashing on
watched message event. -Process= "RTTYS Process", ipl= 5, pid= 78 -Traceback= 410545B0
41054694 418628A8
```

Conditions: This symptom is observed on a Cisco 6509 switch running Cisco IOS Release 12.2(18)SFX6.

Workaround: There is no workaround.

- CSCtg69202

Symptoms: CUBE modifies the RTP port number before passing it to the remote end, which causes one-way audio.

Conditions: This symptom is observed only when the RTP port number is higher than the RTCP port number in the incoming request from the endpoint. Instead of sending the same RTP port number, CUBE decrements the RTP port number by one less than the RTCP port number when it forwards the OLC Ack to the destination side. This causes the destination to send the audio packets to the wrong port on the originating side, causing one-way audio.

Workaround: There is no workaround.

Further Problem Description: Under some specific conditions, when CUBE receives the OLC acknowledgement with the media control information from an H323 client, instead of passing the same RTP port number to the remote end, it modifies the RTP port number, causing the one-way audio.

- CSCtg71332

Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

Workaround:

1. Use SP services feature set.
 2. Upgrade router to Cisco IOS Release 12.4(24)T.
 3. Install one or more PVDM sLOTS.
- CSCtg76688

Symptoms: An active Cisco route processor reloads in a scale scenario (16k - 24k sessions) when the **clear subscriber session all** command is entered.

Conditions: This symptom is observed only when there are 16k-24k sessions and the **clear subscriber session all** command is entered.

Workaround: Do not enter the **clear subscriber session all** command when more than 16k sessions are up on the router.

- CSCtg83932

Symptoms: “Encapsulation aal5auto” may not be enabled under svc mode.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(01.14)T.

Workaround: There is no workaround.

- CSCtg84649

Symptoms: EIGRP is not forming adjacencies over virtual interfaces in a DVTI environment.

Conditions: This symptom is observed on a Cisco ASR 1000 platform with Cisco IOS Release 12.2(33)XNE or Release 12.2(33)XNF1.

Workaround: Remove the passive-interface configurations for Virtual-Template and then re-configure the passive-interface designation. For example,

```
Router#sh run | b router router eigrp 100 network 10.1.0.0 0.0.31.255
passive-interface default no passive-interface Virtual-Template1
Router(config)#router eigrp 100 Router(config-router)#no passive-interface default
Router(config-router)#passive-interface default Router(config-router)#no passive
Virtual-Template 1
```

- CSCtg86714

Symptoms: The **show cellular 0** command might not show any output.

Conditions: The symptom is observed with the **show cellular 0** command.

Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the “MODEM UP” line, you get “LINK UP” and still retain the **show cellular stats**.

- CSCtg87775

Symptoms: The router may unexpectedly reload.

Conditions: The symptom is observed under circumstances where a Cisco 7600 series router is configured to handle several hundred or more neighbors, and an administrator issues the command: **clear bgp vpnv4 unicast ***.

Workaround: Clear individual neighbors separately, limiting yourself to 100 or fewer in any scanner interval.

Further Problem Description: Issuing other clear commands and forcing a switchover between active and standby at during the interval immediately before and after issuing the BGP clear command increases the probability of a reload.

The number of neighbors where this is documented as happening is 1200, but the exact minimum number of neighbors needed to trigger the problem is not documented.

- CSCtg88766

Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

Workaround: There is no workaround.

- CSCtg91201

Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

Workaround: There is no workaround.

- CSCtg91336

Symptoms: A Cisco router may crash during show command **show ip ospf rib** execution.

Conditions: This symptom is observed in Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

- A user enters the **show ip ospf rib** command and stops in the middle.
- The OSPF local rib is significantly changed; for example, routes are removed.
- A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

Workaround: Do not enter the **show ip ospf rib** command. If it is necessary to use the command, enter **terminal length 0** and print the entire output.

- CSCtg92783

Symptoms: Uplink performance degrades by about 70% with HWIC-3G-CDMA when bound to external dialer interface when compared to using cellular interface legacy DDR.

Conditions: This symptom is seen on live network when performance is measured using latency sensitive Internet speed test application.

Workaround: Use cellular interface without binding to external dialer.

- CSCtg94250

Symptoms: Removing **address-family ipv4 vrf <vrf>** (in router BGP) followed by **no ip vrf <vrf>** (where “vrf” is the same) could result in a crash.

Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

1. **no address-family ipv4 vrf <vrf>**
2. **no ip vrf <vrf>**
3. **ip vrf <vrf>**

The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).
 2. Give sufficient time for (1) to complete before applying (2).
- CSCtg95618
Symptoms: 1. MSCD_StartStop fail message is observed in usbflash_mscd_scsi_listener 2. USB flash file system is not accessible sometimes.
Conditions: This symptom is observed on Cisco 892F and C892FW series routers with two USB slots when the USB sticks are removed and swapped. This symptom is not observed when a single USB stick is removed or inserted in a different bus.
Workaround: There is no workaround.
 - CSCtg95940
Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.
Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.
Workaround: There is no workaround.
Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.
 - CSCtg96518
Symptoms: Fast memory leak occurs in CCSIP CCB Pool.
Conditions: This symptom is observed on a Cisco 2951 integrated services router with Cisco IOS Release 15.1(1)T.
Workaround: Reload the router.
 - CSCtg96630
Symptoms: A Cisco router crashes when the user tries to configure a default policy with rsvp group percentage configuration.
Conditions: This symptom is observed when the user tries to configure a default policy with rsvp group percentage configuration under a virtual template.
Workaround: There is no workaround except to avoid this configuration command.
 - CSCtg98783
Symptoms: Cube: call leg 1 receives SDP 101, 0-15; Cube: call leg 2 sends SDP 101, 0-16. This is seen as a different media, and is treated as such.
Conditions: This symptom is observed when Cube is configured in DO-EO with flow-around.
Workaround: There is no workaround.
 - CSCtg99114
Symptoms: The following error message with traceback is observed:

```
%IPC-5-REGPORTFAIL: Registering Control Port
```


Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.
Workaround: Drop IPC traffic using control-plane policing:

```
class-map match-all ipc match access-group name ipc policy-map drop-ipc class ipc drop
ip access-list extended ipc permit udp any any eq 1975 control-plane service-policy
input drop-ipc
```

- CSCth01394

Symptoms: On a Cisco 7606 router that is running Cisco IOS Release 12.2(33) SRD3 with SIP200/SPA-4XCT3/DS0, when you have ppp multilink interface(s) configured with member links from same SPA (software based multilink) and you physically remove SPA, you will see that upon executing the **show ppp multilink** command, the multilink interface still has reference for member links. If you do the **sh run int serialx/y** command, you will get message interface not found.

Conditions: This issue is consistently reproducible.

Workaround: There is no workaround.

- CSCth01939

Symptoms: IPsec packets are dropped on the router and an error is displayed on the console.

Conditions: This symptom is observed on a Cisco IAD2430 with VPN/GRE tunnel configuration and AES256 encryption.

Workaround: There is no workaround.

- CSCth02725

Symptoms: There is an interoperability issue between a third-party vendor's routers and Cisco routers with severe IPTV service failure in Prune-Overriding environment.

Conditions: The symptom is observed in the following scenario:

1. Router A is Cisco 7609 router (IP address 10.1.1.1) and connects to Router B (third-party vendor's router; IP address 10.1.1.3) and Router C (IP address 10.1.1.2).
2. If subscriber under Router C disappears, Router A receives "Prune" message from Router C.
3. Router A does not change "source IP of PruneEcho message (10.1.1.2)" and sends it to Router B.
4. At this time, Router B should send overriding-join to Router A because Router B still has subscribers. But Router B drops the PruneEcho message because source IP (10.1.1.2) is not from PIM neighbor. Router B cannot send overriding-join to Router A.
5. As a result, multicast traffic (IPTV stream) to Router B stops.

Workaround: Connect C and B to become PIM neighbors. However, this cannot always be considered a recommended workaround because of potential high cost and/or other (sometimes third-party) limitations.

- CSCth02789

Symptoms: System can crash when attempting to schedule an IPv6 icmp-echo operation.

Conditions: The symptom is observed with IPv6 and icmp-echo.

Workaround: There is no workaround.

- CSCth03022

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>.

- CSCth03379

Symptoms: A Cisco router reloads while booting with DSL configurations.

Conditions: This symptom is observed on a Cisco router with Cisco IOS Release 15.1(1.15)T configured with DSL controller.

Workaround: There is no workaround.

- CSCth04193

Symptoms: A Cisco router crashes at cce_dp_named_db_http_free_token_info.

Conditions: This symptom is observed when Zone-based Policy Firewall is configured to inspect HTTP traffic.

Workaround: Do not use deep packet inspection.

- CSCth04945

Symptoms: A Cisco router crashes when adding or removing a QoS policy from an interface.

Conditions: This symptom is observed when the following occur:

- packets keep hitting the interface from which the policy is being removed
- the QoS policy is at least a two-level policy
- before the policy was removed, the CLI generated an error for some invalid configuration change in that policy; for example,

```
3845-AA2205(config)#policy-map VOICE-OUT-PARENT 3845-AA2205(config-pmap)#class
class-default 3845-AA2205(config-pmap-c)#no shape average 100000000 Queueing must be
removed from child classes before queueing can be removed from class-default
```

Workaround: Avoid invalid configuration changes in the QoS policy before adding it to or removing it from an interface.

- CSCth05778

Symptoms: Router is showing memory leaks.

Conditions: The symptom is observed when the remote end is sending LCP conf_req messages to a Cisco 10000 series router more frequently (1 per 4 msec) than the normal scenario (1 per 2 seconds).

Workaround: Shut down the PPP link that is flapping.

- CSCth06812

Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:

```
R1(config)#parser view SUPPORT R1(config-view)# secret cisco R1(config-view)#
commands exec include ping R1(config-view)# commands exec include configure terminal
R1(config-view)# commands exec include show ip ospf neighbor <--Where we see the hang
```

Workaround: Do not configure **commands exec include show ip ospf neighbor** command in parser view configuration.

- CSCth07787

Symptoms: A standby device crashes when attempting to configure login banner on the active device.

Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C

Workaround: Use any delimiters other than the following: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C

- CSCth08505

Symptoms: PPPoE sessions may not sync to the standby-RP.

Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

Workaround: Reloading the standby-RP may resolve this issue.

- CSCth09876

Symptoms: Cisco IOS IP Service Level Agreements (SLAs) cannot be auto-discovered if IP SLAs are removed from the responder first.

Conditions: This symptom is observed on a Cisco device after IP SLAs have been unconfigured. Subsequent attempts to reconfigure the device as an IP SLAs responder fail.

Workaround: Reload the router and configure the device as an IP SLAs responder.

- CSCth10764

Symptoms: PPP Negotiation not working correctly between Cisco GSR XR and Cisco 7200.

Conditions: Max-header size different on both ends, PPP not negotiating lower size.

Workaround: There is no workaround.

- CSCth11747

Symptoms: When a switchover occurs with GR enabled, sometimes the NSF states are not preserved and the forwarding entries are lost, leading to packet loss for a few seconds.

Conditions: This symptom is observed only with single sessions with GR configured when the restarting neighbor does a passive open. Chances of hitting this are low since this issue occurs because we receive a new open message before the old tcp session has a chance to reset.

Workaround: Configuring multi-session capability on the neighbor sessions or restricting the restarting neighbors connection to active mode would prevent this issue.

Further Problem Description: When an established session already exists between the GR-enabled routers, and the tcp has not yet notified of reset due to neighbor SSO, if the receiving router gets a new open from the restarting router, as per the RFC it is supposed to tear down the old session and accept the new connection. The old session was being torn down properly but it would take the service reset walker to completely free the session. In case of multi-sessions there was no problem in accepting the new session since multiple sessions are allowed. But in case of a single session that already exists, the new sessions are not allowed until the old session is completely freed. Hence, the new session was getting rejected and notification was sent to the restarting neighbor. The restarting neighbor, upon reception of this notification, would clear the NSF preserve bits and further opens would clear the NSF states on the receiving neighbor and hence the problem. The solution would be to accept the new connections in single session support neighbors when the GR reopen has marked the session for reset and de-linked the topologies. The topologies would be added to the new session and the connection accepted. The old session would be freed when service reset walker is invoked. So, for a transient period of time between the session mark reset and the session free, there would be multiple sessions established on the neighbor even though the neighbor was configured as single session. Dependent DDTS CSCtd99802 and CSCth90239 need to be committed along with this fix to ensure complete working of this functionality.

- CSCth13153
Symptoms: An incorrect UDLR Reporter exists on a router that is connected to a UDLR link and PIM-SM domain with auto-rp configurable.
Conditions: This symptom is observed on a Cisco 7200 series router with Cisco IOS Release 15.1(1.16)T0.1.
Workaround: There is no workaround.
- CSCth15105
Symptoms: BFD sessions flap after unplanned SSO (test crash).
Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.
Workaround: There is no workaround.
- CSCth15268
Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.
Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit on.
Workaround: Set "llc2 local-window" to 1.
- CSCth15353
Symptoms: Incorrect result codes are displayed in vpdn sys logging. The CDN message for admin down was reported in the syslog as "Result Code=2, Error Code=6" instead of "Result Code=3, Error Code=6".
Conditions: This symptom is observed when a session is cleared by a clear command (for example, **clear interface virtual-access 3.1**).
Workaround: There is no workaround.
- CSCth15518
Symptoms: Ping through ISDN BRI interface fails.
Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.
Workaround: There is no workaround.
- CSCth15519
Symptoms: A Cisco router reloads with "show memory <invalid-address_value>".
Conditions: This symptom is observed on Cisco 1861, 880, and 860 routers.
Workaround: There is no workaround.
- CSCth16011
Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But Pfr will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.
Conditions: Introduce loss to network.
Workaround: There is no workaround.
- CSCth16382
Symptoms: A Cisco device crashes at cce_dp_results_get_class_group_element.

Conditions: This symptom is observed when Crypto is on and QoS pre-classify is not enabled. The crash occurs when configurations are loaded and traffic is run.

Workaround: There is no workaround.

- CSCth18146

Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

Workaround: There is no workaround.

- CSCth18611

Symptoms: A Cisco router crashes.

Conditions: This symptom is observed when configuring dynamic nat under the vrf interface with an existing firewall configuration. This symptom is not observed without the vrf configuration.

Workaround: There is no workaround.

- CSCth18982

Symptoms: BGP sessions flap continuously in a multi-session configuration.

Conditions: This symptom is observed when the same peer under the same address family is configured under different topologies (MTR with GR-enabled setup) with multiple topo-ids.

Workaround: The sessions do not flap if topologies use the same topo-id (tid) for the peers active under different topologies or when GR is not enabled.

- CSCth20704

Symptoms: A Cisco router crashes when policy-map is unconfigured while traffic is flowing.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T1.

Workaround: There is no workaround.

- CSCth21017

Symptoms: Traceback is seen when ISIS adjacency state changes.

Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T1.

Workaround: There is no workaround.

- CSCth23787

Symptom: A Cisco router crashes at “mcast_aaa_send_stop_acct_event.”

Conditions: This symptom is observed while unconfiguring “ipv6 mld join-group FF1E::1” in the client after configuring within 15-20 seconds.

Workaround: Unconfigure, if required, after multicast start record is sent.

- CSCth23814

Symptoms: When using Flexible NetFlow, a traceback or crash can occur.

Conditions: This symptom is observed when a monitor is configured with a flow record that has the “BGP next hop” field configured.

Workaround: Ensure that the “BGP next hop” field is not configured for a flow.

- CSCth25634

Symptoms: The password is prompted for twice for authentication that is falling over to the line password.

Conditions: This symptom is observed when login authentication has the line password as fallback and RADIUS as primary. For example:

```
aaa authentication login default group radius line
```

Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example:

```
enable password <keyword> aaa authentication login default group radius enable
```
- CSCth25698

Symptoms: IPv6 packets are not dropped by the firewall.

Conditions: IPv6 packets are not dropped by the firewall in case of Zone to non-zone.

Workaround: There is no workaround.
- CSCth26441

Symptoms: Non-broadcast Ethernet frames are dropped by the Gig1/0 controller that connects to the NME module.

Conditions: This symptom is observed when xconnect is configured on a subinterface and 802.1q trunking is used to connect to the NME module.

Workaround: There is no workaround.
- CSCth28677

Symptoms: CUD fails to be parsed when it contains 0x00.

Conditions: This symptom is observed on a Cisco router configured for X25 translation with CUD verification.

Workaround: There is no workaround.
- CSCth30815

Symptoms: StopCCN result codes and strings do not match RFC.

Conditions: This symptom is observed when the session is cleared by command or due to some error condition; the result code is not correct.

Workaround: There is no workaround.
- CSCth31271

Symptoms: A Cisco ASR router crashes with next-hop recursive.

Conditions: This symptom is observed after the following tasks are executed:

 1. Configure a route-map with recursive next-hop clause for ip address (for example, 1.2.3.4)
 2. Change the recursive next-hop to ip address (for example, 5.6.7.8)
 3. Apply PBR with this route-map to an interface
 4. Delete the route-map
 5. Shut the interface.

Workaround: There is no workaround.
- CSCth31395

Symptoms: Frame-relay PVC stays in INACTIVE state.

Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

Workaround: There is no workaround.

- CSCth33457

Symptoms: A Cisco IOS router configured with IPSec may reload when receiving encrypted packets.

Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

- ip accounting precedence input
- ip accounting mac-address input
- WCCP -Flexible NetFlow
- BGP accounting
- uRPF -mpls accounting experimental input

Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth33500

Symptoms: NAS port is reported as zero on LNS.

Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

Workaround: There is no workaround.

- CSCth33804

Symptoms: Traffic is dropped at CPP with error message “noipv4route” after RP switchover, and traffic on few sessions is dropped.

Conditions: This symptom occurs when VRF is configured for PPPoE sessions and RP switchover is done with traffic flowing.

Workaround: Do not configure VRF.

- CSCth33949

Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

Conditions: This symptom is observed when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

Workaround: Use the **cle vpdn tunnel l2tp all** command instead.

- CSCth35377

Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

Conditions: This symptom is observed on a GigabitEthernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters: encapsulation dot1Q xxx ip pim sparse-mode.

Workaround: Remove “ip pim sparse-mode.”

- CSCth35620

Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

Conditions: The symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

Workaround: There is no workaround.

- CSCth35780

Symptoms: A Cisco router crashes for the SIP multi-part traffic.

Conditions: This symptom is observed when SIP multi-part traffic passes through a Cisco 7200 router. NAT SIP Multi-part must be enabled as part of the NAT configuration.

Workaround: There is no workaround.

- CSCth36261

Symptoms: A router crashes.

Conditions: This symptom occurs when the router is configured for fax calls (specific to T.37 only).

Workaround: There is no workaround.

- CSCth36740

Symptoms: A router may experience CRC and Runt errors.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2 and when the onboard GigabitEthernet interface is hard-coded to 10mb/full duplex. It is seen with the following routers: Cisco 1900 series, Cisco 2900 series, and Cisco 3900 series.

Workaround: There is no workaround.

- CSCth38699

Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-Group mappings.

- CSCth38711

Symptoms: The first WAAS connection takes longer than one minute to begin transferring data.

Conditions: This symptom is observed during AOIM sync, which occurs once per boot or reconfiguration.

Workaround: There is no workaround.

- CSCth39774

Symptoms: UUT hangs when an eTCDF file is loaded on the router in the latest t_base_1 code base.

Conditions: The symptom is observed when an eTCDF file is loaded on the router, the UUT seems to hang. However, the UUT is actually waiting for user input, and if you enter “#” on the CLI, it will print some error messages about invalid commands and return to CLI.

Workaround: Do not use the eTCDF file to configure the encrypted filter, rather directly enter the commands on the CLI of the router.

- CSCth39877

Symptoms: No VPDN logging occurs for the L2TP tunnel.

Conditions: This symptom is observed when the tunnel goes down.

- Workaround: There is no workaround.
- CSCth40090

Symptoms: A Cisco device crashes when initiating an analog CAMA call.

Conditions: On initiation of an analog CAMA call, a crash occurs due to memory corruption leading to a breakpoint exception. A crash occurs in scenarios where e911 is enabled or disabled.

Workaround: There is no workaround.
 - CSCth40213

Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

Workaround: There is no workaround.
 - CSCth40506

Symptom: A Cisco voice gateway does not have its GigabitEthernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

```
-- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
```

Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

```
--May 4 17:49:29.120 GMT=+1: ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry:
Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
```

The call, however, is not cleared from the PRI.
 - CSCth42594

Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

Conditions: The symptom is observed with the following conditions:

 - When multilink is bundled with more than one serial interfaces (not seeing this issue with only one serial interface).
 - Seeing this issue from 1500 and above (not seeing this issue when configure and remove “ppp multilink mrru local 1499”).

Workaround: There is no workaround.
 - CSCth42798

Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

Workaround: There is no workaround.
 - CSCth42999

Symptoms: Serial HWICs (HWIC-4T/4AS/8AS/4A/16A) are not functional after the commit of CSCth18756 (FPGA firmware compressed within IOS image).

Conditions: The symptom is observed when you plug the serial HWIC into the eHWIC slot of the router and test the ping for that particular serial interface.

Workaround: There is no workaround.

- CSCth45623

Symptoms: A memory leak occurs in cce dp reclass.

Conditions: This symptom is observed with WAAS Express plus QoS preclassify disabled plus Crypto plus crypto-map.

Workaround: There is no workaround.

- CSCth45731

Symptoms: PPPoE sessions get synced partially to the standby RP and later never get cleaned up. The **show** command for the sessions looks on a standby RP like the following:

```
Sby#show ppp all Interface/ID OPEN+ Nego* Fail- Stage Peer Address Peer Name
-----
0xB400008A LCP+ CHAP+ IPV6CP+ Undefined 0.0.0.0
```

Peer address is 0 and interface will show the PPP handle instead of the virtual interface of PPP.

Conditions: This symptom is seen when IPCP is getting renegotiated and terminated before the full session sync is done for the upcoming PPPoE session.

Workaround: There is no workaround.

- CSCth46540

Symptoms: Configuring **memory-size iomem** returns an error:

```
Maximum IO percent supported for 2560MB memory is 0 (0MB)
```

Conditions: The symptom is observed on a Cisco 1941 installed with 2.5 GB of DRAM.

Workaround: There is no workaround.

- CSCth46888

Symptoms: When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.

Conditions: The symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.

Workaround: There is no workaround.

- CSCth47765

Symptoms: Once a router boots up, FXS/FXO voice-port in slot2 stays in “S_OPEN_PEND” state. The DSP from the MB that provides resources to the EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards in slot 2 goes into “FW_DNLD_FINISHED” state which causes the voice ports on EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards to go into “S_OPEN_PEND state”.

Conditions: The symptom is observed with Cisco IOS interim Release 15.1(1) T0.9 with 26.8.0 DSPware.

Workaround: There is no workaround.

- CSCth48009

Symptoms: Changes to IOS-WAAS syslog messages.

Conditions: The symptom is observed with syslog messages for IOS-WAAS.

Workaround: There is no workaround.

- CSCth48457

Symptoms: A crash is seen at qos_classify_opttype.

Conditions: The symptom is observed when changes are being made to the service policy while traffic is running. It is seen when using the same child policy-map in multiple classes of the parent and then removing the child policy-map by unconfiguring the parent classes. It happens with the following Cisco IOS Releases: 12.4(15)T, 12.4(20)T, 12.4(22)T, 12.4(24)T, 15.0(1)M, and 15.1(1)T.

Workaround 1: Define the policy-map you wish to run before applying it on the interface level.

Workaround 2: Do not use the same child policy in multiple classes of the parent.

- CSCth49421

Symptoms: Transparent bridging stops working.

Conditions: The symptom is observed when the interface goes to standby from active. The output of **show controllers gigabitethernet slot/port** shows these fields (at the end of output):

When working:

Software filtered frames: 0 Unicast overflow mode: 1 <-- Multicast overflow mode: 1 Promiscuous mode: 1 Total Number of CAM entries: 8 Port Stopped: N

When not working:

Software filtered frames: 0 Unicast overflow mode: 0 <-- Multicast overflow mode: 1 Promiscuous mode: 1 Total Number of CAM entries: 4 Port Stopped: N

Workaround: Remove bridging and reconfigure it on the interface.

- CSCth50479

Symptoms: With high rate of session churn, the **show subscriber sessions** command shows sessions are stuck in the “Attempting” state. The **show subscriber stat detail** command shows that these sessions are actually stuck in the “installing-config” state.

Conditions: The symptom is observed with a high rate of PPP session churn and with a large number of sessions (resulting in more than 70% IOS memory used).

Workaround: Router reload is required to clear stuck sessions.

- CSCth50550

Symptoms: A Cisco device crashes when using PDP filter.

Conditions: This symptom is observed when PDP filter is applied in a QoS Policy.

Workaround: There is no workaround.

- CSCth51125

Symptoms: PCEX-3G-HSPA-R6 is not recognized at bootup:

```
%CISCO800-2-MODEM_NOT_RECOGNIZED: Cellular0 modem not RECOGNIZED. Carrier id not
available or invalid! Replace it with Cisco supported modem and reload the router.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
%CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
```

Conditions: The symptom is observed on a Cisco 881G-K9 that is running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCth52485

Symptoms: A call from the PSTN reaches an AC agent via the AC Route Point and the call is successfully answered. The AC agent then attempts a blind transfer using the AC to another IP Phone, but after around eight seconds of silence the call is dropped.

On the CUBE we see the following (the below messages exclude the communication between the CUCM and the CUBE as it is irrelevant):

```
-Invite outbound to the PGW -200 OK inbound from the PGW -ACK outbound to the PGW
-UPDATE outbound to the PGW -200 OK inbound from the PGW -Invite outbound to the PGW
-200 OK inbound from the PGW -ACK outbound to the PGW -Invite outbound to the PGW -491
Request Pending inbound from the PGW -ACK outbound to the PGW
```

Then the CUBE receives a BYE after 8 seconds from the CUCM and forwards this to the PGW and the call terminates. After receiving the 491 Request Pending, the CUBE is not forwarding this to the CUCM, whereas all previous SIP messages are forwarded successfully. The CUBE should forward this 491 to the CUCM and then the CUCM should react by sending the Invite again for which it received the 491 Request Pending.

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T.

Workaround: There is no workaround.

- CSCth52720

Symptoms: With client-initiated L2TPv2, IPCP packets are not sent when MLP is enabled.

Conditions: The symptom is observed when PPP multilink is configured with Cisco IOS Release 12.4(24)T3, Release 12.4(11)XJ, and Release 15.1(1)T.

Workaround: Remove the PPP multilink configuration or use Cisco IOS Release 12.3(14)T6.

- CSCth55579

Symptoms: Router reloads at clean_out_RA_certs after enrolment with CA server.

Conditions: The symptom is observed after enrollment with CA server.

Workaround: There is no workaround.

- CSCth57478

Symptoms: When configuring SIP digest authentication, user names with more than 25 characters are truncated in the running config and cause the password component to be corrupted. This error is saved through to startup configuration, causing the authentication to be lost on reboot.

Conditions: This symptom is observed with a normal dial-peer configuration on a POTS dial-peer running Cisco IOS Release 15.1(1)T.

Workaround: There is no workaround.

- CSCth57542

Symptoms: The command **show voice dsp command history 1/1:0** reloads a Cisco AS5400XM router if the T1 controller is seated in slot1.

Conditions: The symptom is observed with Cisco IOS Release 15.1(2)T.

Workaround: Apply the **show voice dsp command history** command only for the slots having PVDM2 [C5510] DSPs.

- CSCth58283

Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

Conditions: NAT is enabled.

Workaround: There is no workaround.

- **CSCth59123**
Symptoms: QoS policy may not match traffic after a reload. All packets match class-default.
Conditions: The symptom is observed after you reload the router with QoS policy.
Workaround: Remove and reapply QoS policy.
- **CSCth59217**
Symptoms: Firewall sessions are not seen when ZBFW and gatekeeper are configured on the UUT.
Conditions: The symptom is observed when ZBFW and gatekeeper are configured on the UUT.
Workaround: There is no workaround.
- **CSCth59784**
Symptoms: Process watchdog timeout crashinfo file not written into flash for Cisco 887 router.
Conditions: The symptom is observed on a Cisco 887 router.
Workaround: There is no workaround.
- **CSCth61759**
Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate video stream.
Conditions: There are a couple of scenarios where this problem was observed.
Scenario 1: This problem was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:
7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server
 1. Call is originated by 7985
 2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP "200 OK" response

```
m=video 53722 RTP/AVP 96 97 34 31 b=AS:1920 a=rtpmap:96 H264/90000 a=fmtp:96
profile-level-id=42e016;max-mps=108000;max-fs=3600 a=rtpmap:97 H263-1998/90000
a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1 a=rtpmap:34 H263/90000 a=fmtp:34
CIF4=1;CIF=1;CIF=1;QCIF=1 a=rtpmap:31 H261/90000 a=fmtp:31 CIF=1;QCIF=1 a=sendrecv
```
 3. CUBE sets video m-line to 0 in the SDP of the SIP "ACK" response

```
m=video 0 RTP/AVP 96
```  
Scenario 2:
End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).
CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA
Workaround: There is no workaround.
- **CSCth61827**
Symptoms: Invalid memory action followed by traceback when traffic is on.
Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(2.5)T.
Workaround: There is no workaround.
- **CSCth62854**
Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.
Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.
Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

Workaround: There is no workaround.

- CSCth64507

Symptoms: Bulk Sync failure is seen on redundancy force-switchover command when eem policy is configured and only when the policy file is present in active module.

Conditions: This issue is observed only when the policy file is present in the active and not in the standby module.

Workaround: Have the policy file present in both the active and the standby.

- CSCth64589

Symptoms: The memory allocated at bds_create_link_list & udb_create_ds was leaked. The service policy would not be attached on the interface.

Conditions: This symptom is seen in Cisco routers loaded with Cisco IOS version of Release 15.1(2.5)T. This happens in corner case configurations where the parent class map has only one filter, which is a nested class.

Workaround: The following configuration can be modified to make things work.

```
class-map c1 class-map c2 match class c1
policy-map p1 class c2
```

Replace the above configuration as follows:

```
class-map c1
policy-map p1 class c1
```

The results are the same.

- CSCth65072

Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth66177

Symptoms: The standby PRE crash triggers an active PRE crash.

Conditions: The symptom is observed when the standby PRE crashes due to a memory parity error. The standby PRE crash also triggers an active PRE crash due to bus error.

Workaround: There is no workaround.

- CSCth66251

Symptoms: You are not able to configure a policy-map for the second time in a Cisco 860 router. An “internal data base error” message is seen.

Conditions: The symptom is observed when configuring a policy-map for the second time and with a Cisco 860 router.

Workaround: There is no workaround.

- CSCth67608
Symptoms: Some groups are missing in the MLD Proxy cache on the Proxy router.
Conditions: This symptom is observed when ipv6 mld host-proxy is applied with existing multicast routes.
Workaround: Clear the multicast routes using clear ipv6 pim topology after applying ipv6 mld host-proxy.
- CSCth67788
Symptoms: sVTI stops forwarding traffic when a local policy is configured on a device.
Conditions: The symptom has been observed on a router that is running Cisco IOS Release 15.0(1)M1.
Workaround 1: Do not use a local policy.
Workaround 2: Configure “no ip route-cache cef” on the tunnel interface.
- CSCth67811
Symptoms: Acct-Terminate-Cause is set as “nas-error” in Tunnel stop record when admin clear.
Conditions: This symptom is seen with admin clear tunnel using the **clear vpdn tunnel l2tp all** command.
Workaround: There is no workaround.
- CSCth69243
Symptoms: Error messages and tracebacks involving the TCP timer process appear on the console.
Conditions: This symptom is observed with a large volume of traffic over extended periods of time; the exact trigger is unknown.
Workaround: There is no workaround.
- CSCth69361
Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.
Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.
Workaround: There is no workaround.
- CSCth69364
Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.
Cisco has released free software updates that address this vulnerability.
This advisory is posted at
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw>.
- CSCth71349
Symptoms: Some SSS sessions are staying in “attempting” state for a while when using ISG Static Session Creation.
Conditions: The symptom is observed when using ISG Static Session Creation.
Workaround: Stop incoming traffic from subscribers and wait until the sessions recover, then re-apply the traffic.

- CSCth72598

Symptoms: PVC stays inactive after OIR.

Conditions: The symptom is observed while performing an OIR on a core-facing interface.

Workaround: Do not do an OIR.

- CSCth74420

Symptoms: Vtemplate number is not set in virtual access interface before cloning the commands onto the VA.

Conditions: The symptom is observed with any application that requests a VA to be cloned from a VT.

Workaround: There is no workaround.

- CSCth77531

Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU utilization in the BGP-related processes for several hours (more than 2.5).

Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process uses the most CPU; also, the number of routemap-cache entries should be very high.

```
Router# show ip bgp sum
```

```
BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
main routing table version 1228001 604000 network entries using 106304000 bytes of
memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
cache entries using 4565920 bytes of memory
```

Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results, and the issue will not be observed.

- CSCth78630

Symptoms: Call manager or other SAF clients are not able to learn SAF patterns.

On the forwarder, “show eigrp service-family external-client” displays multiple expired client registrations. The keepalive timer on the stale registrations is 0, and the “Client API Handle” is “0”, however the File Descriptor is still listed in the table. See the following example:

```
abi-4506#sh eigrp service-family external-client SAF External Clients Client Label
Client API Handle File Descriptor ABI_SAF_CLIENT1 0 1 ABI_SAF_CLIENT1 0 2
ABI_SAF_CLIENT1 0 3 ABI_SAF_CLIENT1 0 4 ABI_SAF_CLIENT1 0 5 ABI_SAF_CLIENT1 0 6
ABI_SAF_CLIENT1 0 7 ABI_SAF_CLIENT1 0 8 ABI_SAF_CLIENT1 0 9 ABI_SAF_CLIENT1 0 10
ABI_SAF_CLIENT1 0 11 ABI_SAF_CLIENT1 0 12 ABI_SAF_CLIENT1 0 13 ABI_SAF_CLIENT1 0 14
ABI_SAF_CLIENT1 15 15 ABI_SAF_CLIENT1 16 16 abi-4506#
```

Using the **debug voice saf** command or the **debug eigrp service-family [external-client {client|messages|protocol}]** command shows the following traceback:

```
%SCHED-3-STUCKMTMR: Sleep with expired managed timer 229C03BC, time 0xF2968 (4d20h
ago). -Process= "SAF-EC FORWARDER", ipl= 4, pid= 235 -Traceback= 11A14818 11A14E3C
11130E54 109A0594 10997584
```

Conditions: This symptom occurs when a SAF client unregisters/re-registers to a SAF forwarder.

Workaround: Reload the router acting as forwarder and ensure there is no unregister/re-register activity on the client (for example, do not restart publishing/subscribing services, etc.).

- CSCth80893

Symptoms: POE and Air Connect (AC) on a Cisco 892FW router do not work simultaneously. You cannot connect to the AC console when POE is powered on.

Conditions: This symptom is observed on a Cisco 892FW router that has both POE and Air Connect with POE powered on.

Workaround: There is no workaround.
- CSCth82293

Symptoms: ISR-G2 router crashes due to bus error at PC 0x0 with spurious errors and the following message:

```
%ALIGN-1-FATAL: Corrupted program counter
```

Conditions: The symptom is observed with wrong usage of CNS initial and partial configurations mixed with **cns config retrieve** execution.

Workaround: Avoid wrong CNS usage. Consult Cisco for correct CNS usage.

Further Problem Description: Although the issue is seen with a Cisco 2911, it is not specific to the 2900 series alone. It can occur with any router platform.
- CSCth83508

Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

Conditions: The problem is seen when using WSMA to run the **session install** command.

Workaround: Perform the install manually from a VTY session.
- CSCth84995

Symptoms: Router may reload when performing an ISSU upgrade or downgrade.

Conditions: This symptom occurs when performing an ISSU upgrade or downgrade.

Workaround: There is no workaround.
- CSCth85829

Symptoms: On an async tunnel, enabling “ip cef” can introduce latency/packet drop. You will see the following:

 - Packet loss is observed for CEF-switched traffic.
 - Very high latency is seen for successful packets.

Conditions: The symptom is observed when:

 - “ip cef” is enabled.
 - Service-policy is attached to either dialer or async interface.

Workarounds:

 1. Disable “ip cef”.
 2. Remove service policy from async interface.
 3. Use record option for ping from LAN host.
 4. Use a mainline code, for example: Cisco IOS Release 12.4(25).
- CSCth86402

Symptoms: When flapping a WAN interface, the PIM tunnel disappears.

Conditions: This happens when flapping a WAN interface after a few hours of working.

Workaround: Disable multicast routing, then enable it again.

- CSCth87587

Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

Workaround: There is no workaround.

Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth87638

Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

Conditions: The symptom is observed on WIC-based platforms. It was seen originally on a Cisco IAD243x using a HWIC-CABLE-D-2.

Workaround: Manually change the MAC address problem card.

Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- CSCth89241

Symptoms: Router crash with memory corruption pointing to the DNS resolution for IM servers.

Conditions: The symptom is seen with a firewall policy configured with IM inspection and the IM filter was configured with domain names for address resolution.

Workaround: Remove the protocol-info parameter-map attached to the IM match filter.

- CSCth90593

Symptoms: A Cisco Router may crash from a corrupted program counter: “%ALIGN-1-FATAL: Corrupted program counter” from an IPIP call.

Conditions: This symptom is observed only when the router is acting as a voice gateway.

Workaround: There is no workaround.

- CSCth91093

Symptoms: Exact symptom due to memory corruption is unknown at this time.

Conditions: This symptom is observed after an L2TP HA switchover when L2TP retransmission takes a long time.

Workaround: There is no workaround.

- CSCth91984

Symptoms: Standby resets continuously.

Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

Workaround: Unconfigure the **set extcommunity** command.

- CSCth94827

Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima- group on a SONET-ACR controller.

Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

Workaround: There is no workaround.

- CSCth99237

Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

Conditions: The symptom is observed under the following conditions:

1. If the client starts to send LCP echo requests during the PPP Authentication phase.
2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

Workaround: There is no workaround.

- CSCti01692

Symptoms: A Cisco ASR1000 crashes upon show run.

Conditions: This symptom is observed with parser config cache interface enabled.

Workaround: Disable the parser config cache interface.

- CSCti01971

Symptoms: The active router crashes during a switchover in a scaled BFD IPv6 setup.

Conditions: The router is configured with a larger number of IPv6 routes with BFD sessions configured. (The test was done with 500 BFD IPv6 sessions.)

Workaround: There is no workaround.

- CSCti04670

Symptoms: A crash may occur while the system is in flux with iEdge sessions going up and down while at the same time the **show ssm** command is issued on the console.

Conditions: This symptom is seen when issuing the **show ssm** command.

Workaround: Issue the **show ssm** command and then show logging to see the results.

- CSCti04754

Symptoms: PPPoE sessions are stuck at attempting state forever.

Conditions: This symptom is seen when sessions are triggered during SSO time, which get stuck at attempting state.

Workaround: Clear attempting state sessions by the **clear** command from box.

- CSCti05663

Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

Conditions: The symptom is observed in the case of an unnumbered relay.

Workaround: There is no workaround.

- CSCti06686

Symptoms: On a Cisco 2900, the async interface drops all outbound packets.

Conditions: This symptom is observed with data packets that are exiting the async interface through the CEF path.

Workaround: Disable hardware framing under the async interface using the following hidden command:

no ppp microcode

- CSCti07805

Symptoms: Router reloads @sipSPIUpdSrtpSession.

Conditions: This symptom is observed with Cisco IOS Release 15.1(2.3)T during Hold/Resume on a basic SRTP call.

Workaround: There is no workaround.

- CSCti08115

Symptoms: The removal of a port-channel interface associated with **mpls ldp advertise-labels interface Port-channelN** can cause a “config sync” error upon an SSO.

Conditions: The symptom is observed after doing an SSO following the removal of the port-channel interface.

Workaround: Before the SSO, remove the offending advertise-labels command when removing the port-channel command with:

no interface Port-channelN no mpls ldp advertise-labels interface Port-channelN

- CSCti08336

Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are “IN” policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go “Out” of policy.

Workaround: There is no workaround.

- CSCti08811

Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

Conditions: This symptom is observed only with EEM policies.

Workaround: There is no workaround.

- CSCti10016

Symptoms: After the **format** command is run on a 32GB or larger disk, the **show** command displays that only 4GB is free on the device.

Conditions: The symptom is observed when formatting disk that is larger than 32GB in capacity.

Workaround: Use a smaller size disk that has no more capacity than 32GB.

- CSCti10222

Symptoms: The following exceptions are seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of XXXX bytes failed from 0xYYYYYYYY, alignment
# Pool: I/O Free: # Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause:
No Alternate pool -Process= "IGMP Snooping Receiving Process", ipl= #, pid= #,
-Traceback= 0x81E8B6Cz 0x81EB0660z 0x802EC198z 0x802EC8E4z 0x802ED88Cz 0x802F1988z
0x803BBD88z 0x803BBF2Cz 0x8045E5CCz 0x804615F4z
```

```
Can't duplicate packet Can't duplicate packet Can't duplicate packet
```

Conditions: This symptom is observed when VLANs are added while multicast traffic is flowing through the router.

Workaround:

1. Prune the multicast feed that is coming from the respective VLAN using the following command: “switchport trunk allowed vlans except <mcast vlan#>”; or
2. Upgrade to Cisco IOS Release 15.1(2)T1.

- CSCti10518

Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

Workaround: There is no workaround.

- CSCti10726

Symptoms: A Cisco router reloads when it is configured for IPSec tunnel and the **show ip nbar protocol-d top-n** command is entered.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.9)T and configured for IPSec tunnel.

Workaround: There is no workaround.

- CSCti10828

Symptoms: In Cisco IOS Release 12.4T, there is no response to SNMP queries of:

```
1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive 1.3.6.1.4.1.9.9.276.1.1.2.1.12
cieIfHighSpeedReceive
```

within the CISCO-IF-EXTENSION-MIB although supported at the CLI:

```
interface GigabitEthernet0/3 bandwidth receive 100 <<<<<
==> BW 100000 Kbit/sec, RxBW 100 Kbit/sec
```

Conditions: This symptom is observed under normal conditions.

Workaround: There is no workaround.

- CSCti13286

Symptoms: Putting this configuration on a router:

```
router rip version 2 no validate-update-source network 10.0.0.0 no auto-summary !
address-family ipv4 vrf test no validate-update-source network 172.16.0.0 no
auto-summary version 2 exit-address-family
```

and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti15990

Symptoms: EzVPN will not come up if the dialer interface flaps.

Conditions: This symptom is observed when the dialer interface is profile- based.

Workaround: Change the dialer interface to non-profile-based.

- CSCti17190

Symptoms: A router crashes when trying to do sre install.

Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

Workaround: There is no workaround.

- CSCti18510

Symptoms: Skinny phone registration fails when it is connected to a NAT router.

Conditions: The symptom is observed with skinny (SCCP) phone traffic passing through a NAT router (where PAT is configured).

Workaround: There is no workaround.

- CSCti18745

Symptoms: If user has configured http port 80 or default http port, then reboots the router, it will produce invalid connection url with port 0. Later the connection from ACS to CPE might fail.

Conditions: This symptom occurs if user has default http port 80 configured and then reboots the router.

Workaround: Once router is up and running, again configure some port other than 80, and then reconfigure port 80.

```
Router(config)#ip http port 8000
```

```
Router(config)#no ip http port or ip http port 80
```

- CSCti19627

Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

Workaround: Remove “call-park system application”.

- CSCti22091

Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

Conditions: The symptom is observed when PfR is configured with the following conditions:

1. list > application > filter > prefix-list
2. Learn > traffic-class: keys
3. Learn > traffic-class: filter > ACL

Workaround: There is no workaround.

- CSCti22190

Symptoms: The EIGRP autonomous system command does not NVGEN.

Conditions:

```
interface Tunnel2 ip vrf forwarding vpn2 no ip next-hop-self eigrp 10
```

Now configure the address-family ipv4 command under legacy mode. For example:

```
router eigrp 10 no auto-summary address-family ipv4 vrf vpn2 no auto-summary
```

Now show the running configuration; the autonomous system command is not NVGENed.

Workaround: Use the “address-family ipv4 vrf vpn2 autonomous 10” command.

- CSCti24577

Symptoms: System crashes on active or hangs on standby.

Conditions: The symptom is observed when a banner command is in the configuration.

Workaround: Remove all banner commands.

- CSCti25063

Symptoms: Call drops after codec change through midcall INVITE.

Conditions: This issue occurs when both the codec and direction are changed compared to previous negotiated SDP. This is seen when using Cisco Unified Border Element (CUBE) with Cisco IOS Release 15.1(2)T. See the following topology:

```
SIP(1) -- CUBE -- SIP(2)
```

Codec G711 is negotiated. Next on SIP(2) midcall INVITE is received with updated SDP. CUBE detects updated SDP but when sending out INVITE on SIP(1), the SDP still has previous codec G711.

Workaround: There is no workaround.

- CSCti25280

Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

```
**ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
```

Conditions: The symptom is observed when there is also a VWIC installed in the chassis (example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

Workaround: Remove the VWIC.

- CSCti25780

Symptoms: One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

Conditions: This symptom is observed when some of the files are compiled with optimization.

Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- CSCti26202

Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

Conditions: The symptom is observed on a Cisco 3900 series router.

Workaround: There is no workaround.

- CSCti26852

Symptoms: Router crashes at ppp_sip_sw_session_cleanup.

Conditions: The symptom is observed with multilink PPP scaled configurations and with a Cisco 7600 series platform. The crash may be seen following a SPA OIR. The crash decode is:

```
sw_mgr_sm_valid_seg_class (seg_class=0x30343408) at
../xconnect/seg_sw_mgr_util.c:443 #1 0x120ab814 in sw_mgr_get_segtype
(seg_class=0x30343408) at ../xconnect/seg_sw_mgr_util.c:478 #2 0x1435cd2c in
ssf_dp_drop_remove_L2_context (seg1_class=0x30343408) at
../machine/./sss/ssf_switching_registry.regh:173 #3 0x1435d48c in
ssf_dp_remove_dp_only_L2_features (seg_class=0x30343408) at
../sss/ssf_switching_util.c:113 #4 0x11c850f8 in ppp_sip_sw_session_cleanup
(session=0x3a1c54f0) at ../VIEW_ROOT/cisco.comp/ppp/core/src/ppp_sip_switching.c:537
```

Workaround: There is no workaround.

- CSCti27128
Symptoms: A Cisco 2911 router crashes repeatedly when trying to boot up.
Conditions: This symptom occurs when an IPVS module is installed in the NME slot with an SM-NM adaptor in a Cisco 2911 router. The Cisco 2921 is not affected.
Workaround: There is no workaround if the IPVS module is required. Otherwise, the IPVS module can be removed from the Cisco 2911.
- CSCti31984
Symptoms: A Cisco router crashes.
Conditions: This symptom is observed when "Show stats" is used to show an auto ethernet monitor operation.
Workaround: There is no workaround.
- CSCti33461
Symptoms: The shared-line free call queue size is not able to reduce and eventually reaches the maximum limit.
Conditions: The symptom is observed when only one active phone for a shared- line is up or when shared-line is configured for a single SIP phone.
Workaround: Remove shared-line configuration and reconfigure to reset the queue size to 0.
- CSCti34627
Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.
Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.
Workaround: Disable GR.
- CSCti34795
Symptoms: In RA mode, SCEP enrolment requests stay in pending status. They will not time out automatically and cannot be cancelled with the **no crypto pki enroll <tp>**.
Conditions: The symptom is observed when "enrollment mode ra" is configured under the Trust-Point.
Workaround: Do not use RA mode, although in certain environments it is not scalable.
- CSCti35326
The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.
The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.
Cisco has released free software updates that address this vulnerability. A workaround that mitigates the vulnerability is available.
This advisory is available at the following link:
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-nat>
- CSCti41615
Symptoms: Cisco 1941, 2901, 2911, or 2921 platforms disable ECC detection when a DIMM1 is installed. Any DRAM bit errors will not be detected/corrected.

Conditions: The symptom is observed on a Cisco 1941, 2901, 2911, or 2921.

Workaround: There is no workaround.

- CSCti45042

Symptoms: When the **reload warm file flash0:<image>** command is issued on a Cisco 3900e router, the router does not boot the specified image due to “System received a Bus Error exception.”

Conditions: This symptom is observed in a Cisco IOS Release 15.1(2.13)T image when the **reload warm file flash0:<image>** command is issued.

Workaround: There is no workaround.

- CSCti46171

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfbw>

- CSCti47649

Symptoms: A router may crash with the message:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04

Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

Workaround: There is no workaround.

- CSCti48014

Symptoms: A device reloads after executing the **show monitor event <comp> ... all detail** command (where <comp> is an option listed under **show monitor event?**).

Conditions: This symptom is observed if the configurations are done in the order below,

monitor event-trace <comp> stacktrace <depth> monitor event-trace <comp> size <size value>

and any related event gets recorded in between the above two configurations.

Workaround: To avoid the crash, change the order of the above configurations; that is, configure the **size** command first and then configure the **stacktrace** command.

- CSCti48483

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCti50740

Symptoms: RSVP to No-RSVP interworking is not functioning correctly.

Conditions: The symptom is observed when a media high-density transcoder option is enabled but not required.

Workaround: Disable “media high-density transcoder”.

- CSCti54173

Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

Conditions: The symptom is observed on a Cisco 7200 series router.

Workaround: There is no workaround.

- CSCti55261

Symptoms: On a phone button that has an overlay with call waiting DN's configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

Conditions: The symptom is observed on a phone button that has an overlay with call waiting DN's and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

Workaround: There is no workaround.

- CSCti57902

Symptoms: IO memory corruption is seen when the image size expands.

Conditions: The symptom is observed when the image size expands.

Workaround: Leave the IO memory to the default (smart init).

- CSCti58272

Symptoms: A PKI server with the **grant auto trustpoint** command will crash on client re-enrolment if PKI-AAA is enabled on the trustpoint associated with the **grant auto** command.

Conditions: If trustpoint “pki-trustpoint” contains an authorization list PKI- AAA option, and pki-trustpoint is used as the “grant auto trustpoint” option on the PKI server:

```
! crypto pki server ca-server ... grant auto trustpoint pki-trustpoint ... crypto pki
trustpoint pki-trustpoint authorization list aaa !
```

The device crashes whenever a re-enrolment attempt is made to the PKI server.

Workaround: Remove authorization list from the trustpoint (and skip the PKI- AAA process).

- CSCti62226

Symptoms: Voice port(s) that are created with PRI/ds0 configurations are active even after shutting down those ports. Because of this, unconfiguring PRI/ds0 configurations throws an error.

Conditions: The symptoms are observed with Cisco IOS Release 15.0(1)M3 when shutting down the voice-port to unconfigure the controllers.

Workaround: Do **no shut** first then **shut**.

Further Problem Description: If you are running a script for regression which cannot be changed there is no workaround. If it is a user interactive case, the above workaround may help.

- CSCti62267

Symptoms: An IPv6 CEF output is not seen in SP.

Conditions: This symptom is observed when IPv6 is configured on UUT. This symptom is not observed with Ping.

Workaround: There is no workaround.

- CSCti62913

Symptoms: IP SLA repeatedly sends traps.

Conditions: This symptom is observed in Cisco IOS Release 15.1T when IP SLA probes start failing and the router is configured to send traps, as in the following sample configuration:

```
ip sla 1 icmp-echo 10.22.22.22 source-ip 10.11.11.11 threshold 2000 timeout 2000
frequency 3 ip sla schedule 1 life forever start-time now ip sla
reaction-configuration 1 react timeout threshold-type consecutive 3 action- type
trapOnly
```

Workaround: There is no workaround.

Further Problem Description: When reaction condition is reached, a flag should be set and only one probe should be sent. No additional traps should be sent until the flag is set.

- CSCti67447

Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

Conditions: The symptom is observed under the following conditions:

1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2.
2. Enable MPLS LDP GR.

Workaround: There is no workaround.

- CSCti68721

Symptoms: The output of “show performance monitor history interval <all | given #>” will appear to have an extra column part way through the output.

Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

Workaround: If the symptom occurs, repeat the command.

- CSCti69008

Symptoms: When dampening is configured for many VRFs, doing full vpv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

Conditions: Dampening configuration changes for VRFs.

Workaround: There is no workaround.

- CSCti72836

Symptoms: The router crashes when removing an ACL.

Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hashtable.

Workaround: There is no workaround.

- CSCti80904
Symptoms: A router reloads at sec_send_command while booting up.
Conditions: The symptom is observed on a Cisco 887 and a Cisco 888 router.
Workaround: There is no workaround.
- CSCti86169
Symptoms: A device that is acting as a DHCP relay or server crashes.
Conditions: This symptom is observed when the “no service dhcp” command is configured.
Workaround: There is no workaround.
- CSCti90602
Symptoms: The PPTP connection is not getting established when “ip nat outside” is configured on the NAT router. The NAT router is between the client and the server.
Conditions: This symptom is observed only with the PPTP connection; all other traffic works fine.
Workaround: There is no workaround.
- CSCti92798
Symptoms: A Cisco router crashes while configuring http commands with atm.
Conditions: This symptom is observed on a Cisco7200 router running Cisco IOS Release 15.1(2)T.
Workaround: There is no workaround.
- CSCti93398
Symptoms: A Cisco 1861 router reloads.
Conditions: The reload occurs upon booting.
Workaround: There is no workaround.
- CSCti98219
The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:
 - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
 - Session Initiation Protocol (Multiple vulnerabilities)
 - H.323 protocol
 All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.
Cisco has released free software updates that address these vulnerabilities.
This advisory is posted at
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.
- CSCtj06390
Symptom: Ping fails after configuring crypto.
Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.
Workaround: There is no workaround.

- CSCtj07125

Symptoms: Cisco IOS WAAS Express uses the burned-in MAC address of the first Ethernet interface as its own local device ID. This device ID is sent as a router identifier to the WAAS Central Manager (WCM) and is communicated to other WAAS peers during autodiscovery.

On Cisco 1941W platforms, the burned-in MAC address of the first Ethernet interface is 0000.0000.0007, which happens to be the same for all Cisco 1941W routers.

This will cause the WCM to have two routers that are registered with the same client ID. It might also affect IOS-WAAS operation.

Conditions: This symptom is observed while registering WAAS on Cisco 1941W platforms with the WCM and enabling WAAS on these platforms.

Workaround: There is no workaround.

- CSCtj20106

Symptoms: Router crashes upon removing “ip flow monitor” from an interface.

Conditions: The symptom occurs on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(2.19)T.

Workaround: Enable “protocol-discovery” on the interface and then configure “flow monitor”.

- CSCtj20545

Symptoms: When a host behind a ZBF implementation is disconnecting ungracefully and loses the TCP connection information, TCP keepalive sessions will only be terminated on the other endpoint after the TCP keepalive times out. This is because the RST from the host that receives the keepalive segment is getting dropped by the ZBF.

Conditions: The symptom is observed when you have TCP connections using keepalive going over a ZBF implementation.

Workaround: Shorten the keepalive timeout on the other endpoint.

- CSCtj22125

Symptoms: NBAR is not disabled and does not free resources.

Conditions: The symptom is observed when “protocol-discover” is configured and unconfigured.

Workaround: There is no workaround.

- CSCtj25649

Symptoms: Inline power to ip phone fails on NM-16-ESW and NMD-36-ESW

Conditions: This symptom is seen on NM-16-ESW and NMD-36-ESW that is using a Cisco IOS Release 15.1(2)T1.1 image.

Workaround: There is no workaround.

- CSCtj31743

Symptoms: Memory leaks@slaAddSeqNum are seen.

Conditions: This symptom is observed when "pfs border" is configured.

Workaround: There is no workaround.

- CSCtj32574

Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

```
router eigrp 1 redistribute connected no redistribute connected
```

The **no redistribute connected** command is not being backed up to the standby.

Conditions: The symptom is observed with any redistribute-related commands.

Workaround: There is no workaround.

- CSCtj38327

Symptoms: Router crashes due to NBAR configuration.

Conditions: The symptom is observed when **ip nbar protocol- discovery** is applied to the tunnel interface.

Workaround: There is no workaround.

- CSCtj38346

Symptoms: Router crash is seen when configuring the **default transmit- interface** command.

Conditions: The symptom is observed with Cisco IOS interim Release 15.1(2.19)T.

Workaround: There is no workaround.

- CSCtj39664

Symptoms: A router that is running Cisco IOS Release 15.1(2)T1 may crash when attempting to configure Zone-Based Firewall.

Conditions: The symptom is observed when attempting to configure zone-pair. It occurs only with a Cisco 861 router.

Workaround: There is no workaround.

- CSCtj53363

Symptoms: A Cisco router hangs indefinitely and the console does not respond.

Conditions: The symptom is observed with the following conditions:

- AIM-VPN in ISR + ZBFW; or
- A Cisco 2811/2821 Onboard VPN + ZBFW

Once traffic starts, the router hangs within minutes.

Workaround: If the device is a Cisco 2811/2821, use sw crypto + ZBFW.

Alternate Workaround: If the device is a Cisco 2851 or higher ISR, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj76297

Symptoms: Router hangs with interoperability of VM and crypto configurations.

Conditions: The symptoms are seen only during interoperability between video- monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

Workaround: Disable AIM and use onboard CE.

- CSCtj94617

Symptoms: A mem leak occurs when the **show running/ show ip access-list** command is entered.

Conditions: This symptom is observed even without a named ACL configured on the device.

Workaround: There is no workaround.

Further Problem Description: The mem leak occurs in a dynamic list that is not destroyed properly.



Caveats for Cisco IOS Release 15.1(4)M

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M7, page 570](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M6, page 585](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M5, page 605](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M4, page 624](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M3a, page 638](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M3, page 638](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M2, page 655](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M1, page 679](#)
- [Open Caveats—Cisco IOS Release 15.1\(4\)M, page 701](#)
- [Resolved Caveats—Cisco IOS Release 15.1\(4\)M, page 701](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Resolved Caveats—Cisco IOS Release 15.1(4)M7

Cisco IOS Release 15.1(4)M7 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M7 but may be open in previous Cisco IOS releases

- CSCs118054

Symptom: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login and not after unsuccessful login attempts.

Conditions: This symptom occurs on a router running Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCtl90292

Symptom: The following error messages are displayed:

```
an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from
0x42446470, alignment 32 Pool: I/O Free: 11331600 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "BGP I/O", ipl= 0,
pid= 564 -Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
40FD1964 403BDBFC 403BCC34 40344508 403668AC
Show buffers shows: 1. Increased miss counters on the EOBC buffers. 2. Medium buffer
leak
Router#sh buffers Buffer elements: 779 in free list (500 max allowed) 1582067902 hits,
0 misses, 619 created
Interface buffer pools: .... Medium buffers, 256 bytes (total 89647, permanent 3000,
peak 89647 @ 00:01:17): 273 in free list (64 min, 3000 max allowed)
EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400): 0 in free list (0 min, 2400
max allowed) 2400 hits, 161836 fallbacks 1200 max cache size, 129 in cache ....
```

Conditions: This symptom is observed when several hits and failures are seen for medium buffers. All are linktype IPC. For example: Buffer information for Medium buffer at 0x4660E964 ... linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtyp 0 if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)

Also, “show buffers old” shows some buffers hanging on EOBC buffers list for a really long time like a few weeks or more.

Workaround: There is no workaround.

- CSCtn10698

Symptom: CUBE crashes at sipSPI_ipip_free_channel_info_data.

Conditions: This symptom occurs during a glare condition between UPDATE and ReINVITE, that is, Received UPDATE on one leg and Received INVITE on the other leg.

Workaround: There is no workaround.

- CSCtn72925

Symptom: PFR fails to get notified about interface state changes.

Conditions: The issue is seen specifically when using Frame Relay and Multilink Frame Relay subinterfaces as PFR external exits and the main interface flaps.

Workaround: Use the following command:

clear pfr master *.

- CSCtq91305

Symptom: Standby cannot reach HOT sync state with active. The standby RP keeps resetting. The following message is displayed:

*Apr 18 15:38:47.704: %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1),process = IPC Dynamic Cache.

Conditions: This symptom occurs with SSO mode, when the Cisco ASR1k is configured with ISG as dhcp server and with a low dhcp lease timer.

Workaround: There is no workaround.

- CSCtr10577

Symptom: The following error message may be seen:

OCE-3-OCE_FWD_STATE_HANDLE limit reached.

Conditions: This symptom is observed under high traffic.

Workaround: There is no workaround.

- CSCtr88785

Symptom: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts11166

Symptom: A router crashes at cce_dp_ipc_save_feature_objects.

Conditions: This symptom occurs on a Cisco 2951 router running Cisco IOS Release 15.1(2)T1 and Cisco IOS Release 15.1(4)M1.

Workaround: There is no workaround as the trigger of the issue is unknown.

- CSCtw74339

Symptom: Blocked MRIB and SNMP IPC send time outs with no issues in the platform layer.

Conditions: This symptom occurs in a control session when RPC replies using the seat ID as the dest_port and other normal control messages use IPC_SEAT | IPC_CONTROL_PORT_ID as the dest_port. Because of this, 2 messages from the same control session do not match when we receive an acknowledgement for one of them.

Workaround: There is no workaround.

- CSCtx23534

Symptom: The reverse route of an EzVPN client is not being copied over to the HA peer.

Conditions: The symptom is observed when using stateful failover via IPsec HA.

Workaround: Manually add routes for the remote peers into the routing table using static routes.

- CSCtx31177

Symptom: A watchdog crash is seen in avl_search.

Conditions: This symptom is observed under the following conditions:

1. When BFD/REP [pseudo-preemptive processes] is configured in the box.
2. When an interrupt returns a buffer.

Workaround: There is no workaround.

More-Info: The AVL tree of our concern is used to account memory, cpu, buffer usage.

1. A new process is created and we try to add a new entry into the avl tree for accounting.

2. When we are in the middle of inserting an entry into the avl tree, interrupt/pseudo-preemption[PP] happens.
3. Interrupt/PP returns a buffer/allocates memory and then we try to account the buffer usage.
4. To account the buffer, we traverse the AVL tree and end up looping , as the tree is not stable.

- CSCtx56183

Symptom: Router crashes due to block overrun:

```
%SYS-3-OVERRUN: Block overrun at 49156754 (red zone 66616365) -Traceback= 42806C04z
42809B20z 42809D14z 427AD988z 427AD96Cz . . %SYS-6-BLKINFO: Corrupted redzone blk
49156754.... . %SYS-6-MEMDUMP: 0x49156754: 0xAB1234CD 0x12A0000 0x12C 0x44395148
%SYS-6-MEMDUMP: 0x49156764: 0x419B243C 0x49157154 0x49156658 0x800004E8
%SYS-6-MEMDUMP: 0x49156774: 0x1 0x0 0x1000133 0x47D7699C
```

Conditions: This symptom occurs when Websense URL filtering is enabled and long URLs are accessed.

Workaround 1: Disable URL filtering.

Workaround 2: Do not invoke long URLs.

- CSCty59423

Symptom: Memory leak seen with following messages:

```
Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "VOIP_RTCP", ipl= 0,
pid= 299 -Traceback= 0x25B1F0Cz 0x25AB6CBz 0x25B1029z 0x46C02Ez 0x46C89Bz 0x46BCC2z
0x471D12z 0x43EF59Ez 0x43DD559z 0x43DCF90z %SYS-2-MALLOCFAIL: Memory allocation of 780
bytes failed from 0x46C02E, alignment 32
```

Conditions: The conditions are unknown.

Workaround: There is no workaround.

- CSCty80553

Symptom: Multicast router crashes.

Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCtz01126

Symptom: With 2xT1s in an IMA bundle, when a single T1 physical interface receives a hit, unexpectedly the IMA interface flaps even when the second T1 interface is running clean.

Conditions: This symptom occurs in several Cisco 2800 routers which use VWIC2-2MFT-T1/E1 cards and AIM-ATM modules. The routers run on different IOS versions such as Cisco IOS Release 12.4(24)T3, Cisco IOS Release 12.4(15)T13b and Cisco IOS Release 15.1(3)T3.

Workaround: There is no workaround.

- CSCtz12714

Symptom: A Cisco router configured for voice functions may crash.

Conditions: The exact conditions to trigger the crash are unknown at this time.

Workaround: There is no workaround.

- CSCtz13023

Symptom: A crash occurs during registration in SRST mode.

Conditions: This symptom occurs during registration in SRST mode.

Workaround: This issue is fixed and committed.

- CSCtz54775

Symptom: Traffic sourced from a 2901 through a EHWIC-4ESG module resumes forwarding within a maximum of 5 minutes (ARP expiry) instead of 30 seconds (STP convergence time).

Conditions: This symptom is observed after an STP failover occurs.

Workaround: Clear the ARP table of the affected interface (after the VLAN is in a forwarding state).

- CSCua14640

Symptom: The router configuration order changes after the router reloads.

```
BEFORE -----
ntp server 223.168.150.10 ntp server 223.168.151.10
AFTER -----
ntp server 223.168.151.10 ntp server 223.168.150.10
```

Conditions: There are no specific conditions for this symptom.

Workaround: There is no workaround.

- CSCua45206

Symptom: The hub router crashes while removing the Stale Cache entry.

Conditions: This symptom occurs when two spokes are translated to the same NAT address.

Workaround: Spokes behind the same NAT box must be translated to different post-NAT Addresses because this is an unsupported configuration.

- CSCua50247

Symptom: Dropped ping packets on an NM-16ESW module.

Conditions: The symptom is observed with ping packets with a size between 1501-1524 and between NM-16-ESW modules.

Workaround: There is no workaround.

- CSCua70065

Symptom: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

Workaround: There is no workaround.

- CSCua71038

Symptom: A Cisco router crashes.

Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

Workaround: Configure OCSP or CRL but not both

- CSCub04965

Symptom: Multiple symptoms may occur including:

- Multiple sessions established to TACACS+ server which never clear are seen in the output of **show tcp brief**.
- Pings to the loopback address from directly connected equipment suffers packet loss.
- Traffic and pings through the switch suffers packet loss.

- CPU utilization remained stable and below 10% when the issue was occurring, the interface counters were not reporting any errors or drops.
- TACACS+ authentication errors, authorization errors, or accounting errors.
- SSH/TELNET via VTY not accessible.
- If condition exists for a period of time the switch may stop passing traffic.

Conditions: The symptom is observed when the device is configured with TACACS+. It is seen mostly on Cisco 3750/3760 switches, but has been observed on Cisco 6500 switches.

Workaround:

1. Remove the AAA and TACACS+ server configuration.
2. Clear the existing TCP connections with **clear tcp tcb**.
3. Reconfigure the TACACS+ server configuration to use "single-connection" mode.
4. Reconfigure the AAA configuration.

Mitigation using EEM: A Cisco IOS Embedded Event Manager (EEM) policy that is based on Tool Command Language (Tcl) can be used on vulnerable Cisco IOS devices to identify and detect a hung, extended, or indefinite TCP connection that causes the symptoms to be observed. The policy allows administrators to monitor TCP connections on a Cisco IOS device. When Cisco IOS EEM detects hung or stale TCP connections, the policy can trigger a response by sending a syslog message or a Simple Network Management Protocol (SNMP) trap to clear the TCP connection. The example policy provided in this document is based on a Tcl script that monitors and parses the output from two commands at defined intervals, produces a syslog message when the monitor threshold reaches its configured value, and can reset the TCP connection. The EEM script is available at:

<https://supportforums.cisco.com/docs/DOC-19344>

- CSCub12694

Symptom: Interrupt scheduler tracebacks seen.

Conditions: The following are examples of log messages seen:

```
Example 1: %SYS-2-INTSCHED: 'may_suspend' at level 4 -Process= "IP SNMP", ipl= 4, pid=
429 -Traceback= <traceback information> %SYS-2-INTSCHED: 'may_suspend' at level 4
-Process= "IP SNMP", ipl= 4, pid= 429 -Traceback= <traceback information>
Example 2: %SYS-2-INTSCHED: 'may_suspend' at level 2 , all interrupts disabled
-Process= "IP SNMP", ipl= 2, pid= 338 -Traceback= <traceback information>
%SYS-2-INTSCHED: 'may_suspend' at level 2 , all interrupts disabled -Process= "IP
SNMP", ipl= 2, pid= 338 -Traceback= <traceback information> %SYS-2-INTSCHED:
'may_suspend' at level 2 , all interrupts disabled -Process= "IP SNMP", ipl= 2, pid=
338 -Traceback= <traceback information> %SYS-2-INTSCHED: 'may_suspend' at level 2 ,
all interrupts disabled -Process= "IP SNMP", ipl= 2, pid= 338 -Traceback= <traceback
information> %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 16482930.
-Process= "IP SNMP", ipl= 2, pid= 338 -Traceback= <traceback information>
```

In some cases the tracebacks MAY lead to a software forced reload.

Workaround: There is no workaround.

Further Problem Description:

- CSCub30381

Symptom: Router crashes very frequently.

Conditions: The symptom is observed with a router configured with X25 and any dynamic routing protocol.

Workaround: Use static routing instead of dynamic routing.

- CSCub53380

Symptom: Legitimate PPP frames are dropped on an async interface, incrementing both “runs” and “unknown protocol drops” in the **show interfaces** command.

Conditions: This issue is observed with Cisco ISR G1/G2 platforms running Cisco IOS Release 15.x with the following modules.

- HWIC-4A/S
- HWIC-8A/S-232
- HWIC-8A
- HWIC-16A

Workaround: There is no workaround.

- CSCub56842

Symptom: The router stops passing IPsec traffic after some time.

Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in SW.

Workaround: Reload the router before active sessions reach the max value.

To verify, do as follows:

```
router#sh cry eli
CryptoEngine Onboard VPN details: state = Active Capability : IPsec, DES, 3DES, AES,
GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA
IPsec-Session : 7855 active, 8000 max, 0 failed <<<
```

- CSCub82495

Symptom: Serial Interface associated with a Channel-group goes down after a router reload or reboot.

Conditions: This symptom occurs after reload and is applicable to the following:

- HWIC-1CE1T1-PRI
- HWIC-2CE1T1-PRI
- NM-8CE1T1-PRI Line Cards.

Workaround: Do a “shutdown” and “no shutdown” of the corresponding Serial Interface of the channel-group.

- CSCuc09483

Symptom: Under certain conditions, running a TCL script on the box may cause software traceback and reload of the affected device.

Conditions: This symptom occurs when a privilege 15 user may run TCL commands.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.8/3.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C>

No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc10966
Symptom: A router crashes at Process = UNICAST REKEY.
Conditions: This symptom occurs a COOP split and merge.
Workaround: There is no workaround.
- CSCuc41531
Symptom: Forwarding loop is observed for some PfR-controlled traffic.
Conditions: This symptom is observed with the following conditions:
 - Traffic Classes (TCs) are controlled via PBR.
 - The parent route is withdrawn on selected BR/exit.
 Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).
- CSCuc45115
Symptom: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.
Conditions: This symptom is observed in the case where there are two Overlay addresses of a different Address Family on the same NBMA (such as IPv4 and IPv6 over Ipv4). This issue is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.
Workaround: There is no known workaround.
- CSCuc82551
Symptom: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.
Conditions: This symptom is observed with SNMP polling with an IP SLA configuration. The crash signature is as follows:

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE While trying to obtain
the data from IP SLAs Path-Echo (rttMonStatsCollectTable) by SNMP polling operation.
```


Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.
- CSCuc95160
Symptom: After receiving the CRCX message, the Cisco AS5400 does not send 200 ok to SSW. SSW sends the CRCX message to the Cisco AS5400 again. Between these messages, debug outputs are displayed. It seems that the call is not disconnected completely for the end point by the previous disconnect request (the DLCX is received after the CRCX message from SSW). The end point may be stuck in call_disconnecting state.
Conditions: This symptom is observed with MGCP. This issue occurs when the Cisco AS5400 receives DLCX before sending 200 ok for the first CRCX message.
Workaround: There is no workaround.
- CSCud11078
Symptom: Removal of the service instance on the target device causes a crash.

Conditions: Not consistently reproducible on all configurations as the underlying cause is a race condition.

Workaround: De-schedule the probe before removing the service instance.

- CSCud56450

Symptom: PPP drops 20-40 percent of incoming frames.

Conditions: This symptom is observed when using WIC-1B-S/T-V3 or VWIC2-xMFT-T1/E1 in PPP mode on a Cisco c1900/c2900/c3900/c3900e (or ISR G2) router.

Workaround: Use HWIC-4B-S/T (for BRI) or the VWIC3 card (for T1/E1).

- CSCud63381

Symptom: Switching from periodic to on-demand DPDs may cause the DPDs to fail intermittently and thus IPsec failover may not work correctly.

Conditions: This symptom is observed under the following conditions: 1. If you are using Cisco 7200-VSA. 2. For Cisco IOS Release 15.1(4)M2. 3. When on-demand DPDs are configured for IPsec failover.

Workaround: Disable the SCTP session:

```
ipc zone default association 1 shutdown
```

- CSCud65796

Symptom: Encryption stops with VSA upon removing and reapplying tunnel protection on any one of the tunnel interfaces.

Conditions: This symptom occurs in DMVPN with shared IPsec profiles (shared keyword - at least two m-gre tunnels).

Workaround: Perform shut/no-shut on the tunnel interface.

- CSCud67105

Symptom: Virtual-Access is not removed when “clear ip nhrp” or “clear crypto session” are issued or when spoke-spoke FlexVPN session is gone. This is seen only in case of FlexVPN.

Conditions: This symptom is seen only when CSCuc45115 is already in image.

Workaround: There is no workaround.

- CSCud67796

Symptom: No audio and/or no ringback with SIP calls through ZBFW when relying on SIP ALG to open pinholes/pregenerate sessions for RTP.

Conditions: The symptom is observed with the following conditions:

1. ZBFW configured to inspect SIP.
2. No other means to permit RTP traffic in other ZBFW classes/policies.
3. RTP is opened/negotiated/established by SDP in 180 Ringing and SDP in PRACK.

Workaround: Modify ZBFW policy to allow RTP port range through. Either inspect all UDP or write more specific classes to allow RTP between only necessary endpoints.

- CSCud68178

Symptom: The Cisco ASR 1000 series router and Cisco ISR 4400 series hubs crash.

Conditions: This symptom occurs when both the physical and tunnel interface are flapping.

Workaround: There is no workaround.

- CSCud72625

Symptom: Router experiences high CPU due to interruptions and queues when the VSA starts to fill.

Conditions: The symptom is observed with the following conditions:

- Cisco 7200 NPE-G2 with VSA module for encryption.
- Crypto map or tunnel protection mode applied to an interface to send traffic to VSA.

Workaround: Disable the VSA module. The **test pas vsa reset 0 2000** command resets the VSA module.

- CSCud78362

Symptom: Users may experience “no audio” when the router is supposed to be playing IVR (prompt play).

Conditions: This symptom occurs on the Cisco 3925E and Cisco 3945E platforms when there are more than 350 concurrent prompt plays.

Workaround: There is no workaround.

- CSCud86856

Symptom: The router crashes soon after executing “clear policy-firewall sessions”.

Conditions: This symptom is observed with ZBF, and only with a large number of sessions.

Workaround 1: Do not use the **clear firewall-policy sessions** command.

Workaround 2: Increase the IO memory size using “memory-size iomem 25” (use the right percentage depending on your free processor memory) and reload. However, you may still notice CPU hogs when executing “clear policy-firewall sessions”.

- CSCud93758

Symptom: A router crashes due to the following messages:

- SYS-3-CPUHOG
- SYS-2-WATCHDOG

Conditions: This symptom occurs on the ISDN L2 process.

Workaround: There is no workaround.

- CSCue04841

Symptom: When the SM module is removed, a %DXMRVL_FLTMG-7-INTERNAL_ERR output occurs with a traceback and when the SM module is reinserted, and the “switchport mode trunk” command is entered, a crash occurs.

Conditions: This symptom occurs in Cisco IOS Release 15.1(4)M5.

Workaround: There is no workaround.

- CSCue18443

Symptom: Command authorization is denied while entering an access list that includes a host address and a subnet mask.

Conditions: This symptom occurs in Cisco IOS Release 15.1(4)M2.

Workaround: There is no workaround.

- CSCue31321

Symptom: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.

Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.

Workaround: Set “term len 0” before running the **how ip cef ... detail** command.

- CSCue36360

Symptom: The following error message is seen followed by a software forced reload:

```
CMD: 'wr mem' 12:42:12 MST Wed Jan 30 2013 Jan 30 19:42:18.245: %SYS-6-STACKLOW: Stack
for process FTP Write Process running low, 0/6000
```

Conditions: This symptom occurs on a router running Cisco IOS while auto archiving the configuration to a file server.

Workaround: There is no workaround.

- CSCue40304

Symptom: Some senders could not be found in the show ip rsvp sender vrf <vrf_name> command output.

Conditions: This symptom is observed on configuring senders on spokes when using Refresh Reduction.

Workaround: Turn off refresh reduction and clear ip rsvp sender*.

- CSCue43669

Symptom: There is a 2-10% packet loss to hypervisor and VM.

Conditions: This symptom occurs in phase III DMVPN where the spoke contains a UCSE.

Workaround: Use the external interface and remove QoS preclassify from the tunnel. Also, if you use the mod/1 port, this problem will be resolved. In this example ucse4/1 works, but ucse4/0 has drops.

- CSCue48419

Symptom: The Cisco AS5350 stops processing calls on PRI with a signaling backhaul from PGW. In the packet trace, there is no q931message from PGW. Further analysis shows that as5350 sends a q_hold (0x5)message in BSM, causing peer (PGW) to stop sending signaling traffic. However, there is no BSM_resume message or BSM_reset sent after it. Hence, PGW is stuck in this condition. There was earlier defect for CSCts75818 with similar symptoms in U-state.

Conditions: This symptom is observed due to some RUDP timing issues that cause BSM session switchover.

Workaround: Reload the Cisco AS5350 (but only when CU notices the outage). Also, shutting both Ethernet interfaces may help, but this workaround has not been tested.

- CSCue49632

Symptom: TCP closes connection for DLSw peer without calling dlsw_tcpd_fini.

Conditions: The symptom is observed with Cisco IOS Release 15.1(4)M4, dlsw_tcpd_fini is not called and DLSw times out. When you close the remaining TCP connections and the DLSw peer FSM cycles back to disconnected. This issue is seen only when TCP FIN is received.

Workaround: Set the higher IP address on 7206 VXR router.

- CSCue52864

Symptom: When the Output Service policy is applied to the serial links of the HWIC-xCE1T1-PRI card, the serial links bounce. Another symptom is that when a Serial interface has HDLC32 hardware, packet drop is observed in another interface such as GigabitEthernet, when output

queueing policies are applied to both of these interfaces: Serial and GigabitEthernet. The dropped packets can include keepalives for routing protocols such as OSPF, EIGRP, or BGP, and this will result in routing protocol flaps.

Conditions: This symptom is observed with the following conditions:

1. When more than two channel groups are applied to the same controller port.
2. When the serial links are congested.
3. When the Output Service policy is applied to more than two serial links of the same controller port.

Workaround: Do not apply the Output Service policy.

- CSCue54104

Symptom: A crash is seen intermittently.

Conditions: This symptom occurs after 60+ PRI calls take place. The exact conditions are still being investigated.

Workaround: There is no known workaround. Downgrade to Cisco IOS Release 15.1(4)M3 or earlier releases.

- CSCue56272

Symptom: The Cisco ISR crashes due to watchdog timeout after SYS-3-CPUHOG errors with a traceback.

Conditions: This symptom is observed with voice traffic through the router.

Workaround: There is no workaround.

- CSCue59775

Symptom: The device crashes.

Conditions: This symptom is observed when the service-policy is removed.

Workaround: There is no workaround.

- CSCue62292

Symptom: The router crashes with an address error with the following messages before the crash:

```
Di0 DDR: dialer shutdown complete %DIALER-6-BIND: Interface Vi3 bound to profile Di0
%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up %LINK-3-UPDOWN:
Interface Virtual-Access3, changed state to up %DIALER-6-UNBIND: Interface Vi3 unbound
from profile Di0
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x22473FA0
```

Conditions: This symptom is observed when a Dialer interface is unbound.

Workaround: There is no workaround.

- CSCue65130

Symptom: cmCallerID in CISCO-MODEM-MGMT-MIB is not updated when there is no CallerID.

Conditions: This symptom is observed where incoming calls with no CID (Caller-ID) do not update the cmCallerID entry in the CISCO-MODEM-MGMT-MIB. When a call with no CID arrives, the CID from the previous caller stays in the MIB, which leads to an authentication bypass and produces billing errors.

Workaround: There is no workaround.

- CSCue68127

Symptom: A Cisco 3845 router will crash due to IO memory corruption.

Conditions: This symptom occurs when WebVPN is enabled and the router receives a TLS hello packet from the server.

Workaround: There is no workaround.

- CSCue68318

Symptom: The ATM interface and subinterface are up/up but are unable to access the Internet.

Conditions: This symptom occurs only when the IP address of that ATM interface is configured under the EIGRP process.

Workaround: Downgrade to Cisco IOS Release 15.0(1)M8.

- CSCue68761

Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3.

```
Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin
----- show buffers -----
Buffer elements: 156 in free list (500 max allowed) 11839912 hits, 0 misses, 617
created
Public buffer pools: Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @
10:04:00): 0 in free list (20 min, 150 max allowed) 7968057 hits, 202704 misses, 2128
trims, 47265 created 71869 failures (680277 no memory)
----- show buffers usage -----
Statistics for the Small pool Input IDB : Mu1 count: 45180 Caller pc : 0x22CF95C4
count: 45180 Resource User: IP Input count: 45180 Caller pc : 0x22381654 count: 2
Resource User: Init count: 2 Output IDB : Mu1 count: 4 Caller pc : 0x2380114C count: 4
Resource User: PIM regist count: 4 Number of Buffers used by packets generated by
system: 45187 Number of Buffers used by incoming packets:
+++++small buffer packet+++++
<snip>
Buffer information for Small buffer at 0x2A815220 data_area 0xD9DEB04, refcount 1,
next 0x0, flags 0x2080 linktype 7 (IP), encntype 16 (PPP), encsize 2, rxtype 1 if_input
0x30F21520 (Multilink1), if_output 0x0 (None) inputtime 00:02:46.212 (elapsed
05:55:11.464) outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
datagramstart 0xD9DEB56, datagramsize 38, maximum size 260 mac_start 0xD9DEB56,
addr_start 0x0, info_start 0xD9DEB58 network_start 0xD9DEB58, transport_start
0xD9DEB6C, caller_pc 0x22CF0044
source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11, TOS: 192 prot:
17, source port 496, destination port 496
Enter hex value: 0x22CF95C4 0x22CF95C4:ip_mforward(0x22ce9448)+0x51c Enter hex value:
0x22CF0044 0x22CF0044:ip_mforward(0x22ce9448)+0x51c
```

Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3. When IP Multicast is used with NAT, in certain scenarios when NAT functionality returns error, multicast code does not free duplicate packet buffers eventually leading to exhaustion of packet buffer pool in the router.

Workaround: There is no real workaround except to disable NAT.

- CSCue88659

Symptom: When installing a new signature file, a router reports traceback or crash with Cisco IOS-IPS.

Conditions: This symptom occurs when installing a new signature file.

Workaround: There is no workaround.

- CSCue94880

Symptom: RTP traffic fails in reverse direction when an outside source list is configured and RTP SA IP matches against this list.

Conditions: The symptom is observed with a Cisco IOS version above 12.4(9) mainline.

Workaround: Use Cisco IOS Release 12.4(9).

- CSCuf36446

Symptom: Router crashes during processing of the following CLI:

```
(conf) no metadata flow
```

Conditions: The symptom is observed with a moderate scale of metadata flows, using several different interfaces.

Workaround: There is no workaround.

- CSCuf48207

Symptom: Controller SHDSL Group (0) info is in DSL DOWN state:

```
Type: 2-wire g.shdsl, status: Configure Firmware SHDSL wire-pair (0)
```

Conditions: This symptom occurs when the SHDSL line is noisy and the SHDSL controller is struck in GHS_STARTUP state.

Workaround: There is no workaround.

- CSCuf51357

Symptom: An SSLVPN-enabled router crashes repeatedly and TCP process leaks are observed with the following messages:

```
Nov 8 2012 15:23:53: SYS-2-MALLOCFAIL Memory allocation of 1740 bytes failed from
0x2152A990, alignment 128
Pool: I/O Free: 55984 Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause:
No Alternate pool -Process= "encrypt proc", ipl= 3, pid= 301
-Traceback= 23B95D80z 21526538z 21526C70z 21529D10z 23158AE4z 26989D68z 2698B4E4z
2697C780z 2697CD60z 24233A58z 2424D6C8z 2424A25Cz 23B829BCz 23B829A0z
```

Conditions: This symptom occurs due to memory corruption at tcp_ha_sync_estab_connection().

Workaround: There is no workaround.

- CSCuf56842

Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

Conditions: This symptom is observed when the **show pfr master application detail** command is used via SSH.

Workaround: There is no workaround.

- CSCuf78524

Symptom: Pings done with size near to the “ppp multilink fragment size” fails when performed from a device connected to the Cisco 2901 router. However, the ping is a success when performed directly from the router.

Conditions: This symptom is observed when the pings are performed from a device connected to the Cisco 2901 router.

Workaround: There is no workaround.

- CSCuf89865

Symptom: MAC addresses are being learnt from the STP blocking port.

Conditions: This symptom occurs when the STP topology is changed and the FWD port goes to BLK state.

Workaround: Manually refresh the MAC address table through a CLI command.

- CSCuf93376

Symptom: CUBE reloads while testing SDP passthrough with v6.

Conditions: The symptom is observed while testing SDP passthrough with v6.

Workaround: There is no workaround.

- CSCuf93471

Symptom: After a brief unavailability of LDAP CRL, no new CRL fetches can be performed. The following messages are seen on the interface:

```
---- Mar 28 08:23:37.988: CRYPTO_PKI: Retrieve CRL using LDAP DIRNAME Mar 28
08:23:37.988: CRYPTO_PKI: Failed to send the request. There is another request in
progress. ----
```

Conditions: This symptom was first seen in Cisco IOS Release 15.1(4)M6. The issue is not limited to this release.

Workaround: Configure the “revocation-check none” command under the affected trustpoint. Reload the router.

- CSCug25383

Symptom: A memory corruption crash occurs on a router running Cisco IOS Release 15.1(4)M6 or later versions. Crashinfo would contain errors similar to following:

```
%SYS-3-BADMAGIC: Corrupt block at 4B47BC14 (magic EF4321CD) -Traceback= [Omitted]
%SYS-6-MTRACE: mallocfree: addr, pc 4D7D4F0C,41EAA79C 4D7D4F0C,40000294
4D59FAD8,41EAA780 4D59FAD8,4000020A 4B47BC44,44D38F78 4D7D3E3C,44D3B290
4D7D3E3C,4000001E 4D7D1B84,44D3B290 %SYS-6-MTRACE: mallocfree: addr, pc
4D7D1B84,30000042 4D5A2130,60000028 4D5A1F8C,419747BC 4D7D3C00,419855E0
4D7D3C00,40000106 48B2CAF4,41974508 48B2CAF4,400000BA 4D5A0A20,419FDAB4
%SYS-6-BLKINFO: Corrupted magic value in in-use block blk 4B47BC14, words 0, alloc
B0D0B0D, Free, dealloc B0D0B0D, rfcnt 44D3B2FC -Traceback= [Omitted] %SYS-6-MEMDUMP:
0x4B47BC14: 0xEF4321CD 0x41974734 0xB0D0B0D 0xB0D0B0D %SYS-6-MEMDUMP: 0x4B47BC24:
0xB0D0B0D 0xB0D0B0D 0x15A3C78B 0x0 %SYS-6-MEMDUMP: 0x4B47BC34: 0x44D3B2FC 0x4B470408
0xEF4321CD 0x44D38E08
```

Conditions: This symptom occurs in a router running Cisco IOS Release 15.1(4)M6.

Workaround: Downgrade to Cisco IOS Release 15.1(4)M5 or earlier versions.

- CSCug34485

Symptom: Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

Conditions: The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

Workaround: Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf>

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.8/5.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:P/E:H/RL:U/RC:C>

CVE ID CVE-2013-0149 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCug36075

Symptom: Layer 1 on the ISDN PRI does not come up after a reload.

Conditions: This symptom occurs after a reload.

Workaround: Perform a shut/no shut.

- CSCug44667

Symptom: SG3 fax call failures observed for STCAPP audio calls.

Conditions: Fax CM tone detection is turned ON even when all fax and modem related configurations have been disabled on the STCAPP gateway.

Workaround: STCAPP modem pass-through feature can be enabled, but you may run into issues with some answering SG3 fax machines which have stringent requirements for fax CM signal.

- CSCug59650

Symptom: There is an intermittent issue where users will successfully authenticate via Auth-Proxy and download the proxy-acls, but the ACEs do not get applied to the interface ACL resulting in user traffic getting blocked.

Conditions: This symptom occurs when IOS Auth-Proxy is configured on a Cisco 2911 router running Cisco IOS Release 15.1(4)M2. This is an intermittent issue.

Workaround: Clear the auth-proxy session manually or wait for the Auth-Proxy idle timeout to expire.

- CSCug71832

Symptom: I/O memory leaks occur with the following error messages:

```
SYS-2-MALLOCFAIL Memory allocation of 268 bytes failed from 0x6076C1C0, alignment 32
Pool: I/O Free: 3632 Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause:
No Alternate pool -Process= "SCCP Application", ipl= 0, pid= 234 -Traceback= 6082E5B4z
60761188z 607618A8z 60764930z 6237DFA4z 62379CB4z 623873A4z 62373474z 62374E64z
607FAE64z 607FAE48z
```

Conditions: This symptom occurs due to a slow memory leak in the SMALL and MIDDLE buffers.

Workaround: There is no workaround.

- CSCuh23940

Symptom: The line status of the 9th port is up/down for HWIC-D-9ESW in the Cisco 3945 Integrated Services Router. The port status displays down/down in Cisco IOS Release 15.3(1)T1 and Cisco IOS Release 15.1(4)M5.

Conditions: This symptom occurs when the Cisco 3945 Integrated Services Router is used.

Workaround: There is no workaround.

- CSCuh43252

Symptom: After upgrading to Cisco IOS Release 15.0(2)SE3, you can no longer authenticate using TACACS. The TPLUS process on the switch will be pushing the CPU up to 99%.

Conditions: The symptom is observed when you use TACACS for authentication.

Workaround: Downgrade the switch to a version prior to 15.0(2)SE3.

Resolved Caveats—Cisco IOS Release 15.1(4)M6

Cisco IOS Release 15.1(4)M6 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M6 but may be open in previous Cisco IOS releases

- CSCso88138

Symptoms: When there is a link flap or a reload, RSVP shows that the interface is down while actually the interface is up. Because of this, the tunnel may take a backup path even when the interface is up.

Conditions: The conditions for this symptom are unknown at this time.

Workaround: Perform a shut/no shut on the interface.

- CSCsz30049

Symptoms: A router may crash with memory corruption or with one of the two following messages:

```
%SYS-6-STACKLOW: Stack for process HQF Shaper Background running low, 0/6000
%SYS-6-STACKLOW: Stack for process PPP Events running low, 0/12000
```

In the case of memory corruption, a corrupted block will be in an address range very close to process or interrupt level 1 stack (this information is available in the crashinfo file).

Conditions: This symptom is observed on routers running Cisco IOS Release 12.2SB when all of the following conditions are met:

- The router is configured for VPDN/L2TP.
- There is a mixture of PPPoVPDN and “MLP Bundle” users.
- QoS service policy with queuing actions (bandwidth guarantee or shaper) is applied to virtual access interfaces for both types of users.

Here is a way to find out if there are normal PPP users or MLP users:

PPP User via CLI:

```
Router#sh user | inc PPP.*00 [1-9]
Vi4          user#wl-cp03-7k2#4 PPPoVPDN      00:00:00 30.3.0.47
```

MLP via CLI:

```
Router#sh user | inc MLP.*00 [1-9]
Vi8          user#wl-cp04-7k2#5 MLP Bundle    00:00:00 30.4.0.54
```

Workaround 1: Allow only PPPoVPDN (i.e.: prevent “MLP Bundle” creation).

Workaround 2: Disable QoS for “MLP Bundle” users or all users.

- CSCtd67668

Symptoms: A router running Cisco IOS may crash.

Conditions: This symptom is observed with netflow configured on a virtual-template interface.

Workaround: There is no workaround.

- CSCtg82170

Symptoms: The IP SLA destination IP/port configuration changes over a random period of time. This issue is hard to reproduce but has been reported after upgrading to Cisco IOS Release 15.1(1).

So far, it only seems to have affected the destination IP and port. The destination IP may be changed to an existing destination IP that has already been used by another probe. The destination port is sometimes changed to 1967 which is reserved for IP SLA control packets. Other random destination ports have also been observed to replace the configured port for some of the IP SLA probes. Each time when the change happens, many of the IP SLA probes will stop running.

Conditions: This symptom is observed in Cisco IOS Release 15.1(1)XB and Cisco IOS Release 15.1(1)T. Other Cisco IOS versions may also be affected.

Workaround: A possible workaround is to downgrade to any Cisco IOS versions older than Cisco IOS Release 15.1.x.

- CSCti51196

Symptoms: SSH to any IPv6 link-local address connects to itself.

Conditions: This symptom is observed when you configure SSH and try to connect to any link-local address using SSH.

Workaround: There is no workaround.

- CSCtj95182

Symptoms: Scanning for security vulnerabilities may cause a High CPU condition on the Cisco Catalyst 3750.

Conditions: This symptom occurs when a network scanner runs against the Cisco Catalyst 3750 running Cisco IOS Release 12.2.55.SE.

Workaround: There is no workaround.

Additional Information: Vulnerable versions:

- Cisco IOS Release 12.2(52)EX through Cisco IOS Release 12.2(55)SE4.
- Cisco IOS Release 15.1(3)T through Cisco IOS Release 15.1(4)XB8a.
- Cisco IOS Release 15.2(1)GC through Cisco IOS Release 15.2(3)XA.

First fixed in: Cisco IOS Release 12.2(55)SE5, Cisco IOS Release 15.0(1)EX, Cisco IOS Release 15.1(1)SG, Cisco IOS Release 15.2(1)E, Cisco IOS Release 15.2(4)M, and Cisco IOS Release 15.3(1)T.

In the meantime, Cisco published several security advisories for Smart Install vulnerabilities:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smartinstall>

- CSCtl88673

Symptoms: Enhancements to GDOI processing.

Conditions: The conditions for this symptom are unknown at this time.

Workaround: There is no workaround.

- CSCtl99174

Cisco IOS Software contains a memory leak vulnerability that could be triggered through the processing of malformed Session Initiation Protocol (SIP) messages. Exploitation of this vulnerability could cause an interruption of services. Only devices that are configured for SIP inspection are affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP inspection.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-cce>

- CSCtn08613

Symptoms: A Cisco router crashes when interfacing with UCCX.

Conditions: This symptom has been experienced on a UC560 running Cisco IOS Release 15.1(2)T2 when making consult transfer calls.

Workaround: There is no workaround.

- CSCtn15610

Symptoms: Cisco IOS may crash with a bus error accessing addr=0x0 after DSP reset.

Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T13a engineering special and Cisco IOS Release 12.4(24)T4.

Workaround: There is no workaround at this time.

- CSCtn16281

Symptoms: Mesh AP crashes on BVI restart by DHCP.

```
*Feb  9 04:00:45.911: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor 0021.1bc0.XXXX VIDB
Virtual-Dot11Radio2 dot1x control
```

```
*Feb  9 04:01:03.199: %DHCP-5-RESTART: Interface BVI1 is being restarted by DHCP
```

```
*Feb  9 04:01:06.023: %MESH-6-CAPWAP_RESTART: Mesh Capwap re-started
```

```
=== Start of Crashinfo Collection (04:01:06 UTC Wed Feb 9 2011) ===
```

Conditions: This symptom is a corner case and is a low probability crash.

Workaround: There is no workaround. AP will reload and rejoin the controller.

- CSCtn81231

Symptoms: Multicast traffic is not forwarded out of the RBE interface due to incomplete multicast adjacency.

Conditions: This symptom is seen on an ATM DCHP host that is running IGMPv2 that is established over RBE interface to router. Multicast group join is successful. However, multicast adjacency is incomplete and therefore cannot forward multicast traffic.

Workaround: Use the **shutdown** command followed by the **no shutdown** command on the ATM main interface.

- CSCto87436

Symptoms: In certain conditions, an IOS device can crash, with the following error message printed on the console:

```
"%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc"
```

Conditions: This symptom occurs if an SSH connection to the Cisco IOS device is slow or idle.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C>

CVE ID CVE-2012-5014 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq14253

Symptoms: Joins/registers not forwarded to the RP when first configured.

Conditions: This symptom is observed when the router is first configured.

Workaround: Reload all routers in the setup.

- CSCtq17444

Symptoms: A Cisco AS5400 crashes when performing a trunk call.

Conditions: The following conditions are observed:

- Affected Cisco IOS Release: 15.1(3)T.
- Affected platforms: Routers acting as voice gateway for H.323.

Workaround: There is no workaround.

- CSCtq23960

Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

show flash: all

```
-#- --length-- -----date/time----- path
<<snip>>
2          0 Mar 13 2011 09:40:36 crashinfo_<date>
3          0 Mar 13 2011 12:35:56 crashinfo_<date>
4          0 Mar 17 2011 16:14:04 crashinfo_<date>
5          0 Mar 21 2011 05:50:58 crashinfo_<date>
```

Conditions: This symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

Workaround: There is no workaround.

- CSCtq41512

Symptoms: After reload, the ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to Multi-frame established.

Conditions: This symptom occurs when “voice-class busyout” is configured and the controller TEI comes up before the monitored interface.

Workaround: Remove the “voice-class busyout” configuration from the voice-port.

- CSCtq51039

Symptoms: Traffic is dropped with VFR + Cisco Wide Area Application Services (WAAS).

Conditions: This symptom is seen when a flow with fragmented packets is placed in pass through, either because of configuration or because max flows in WAAS is reached. Fragmented packets can occur in the network for a wide variety of reasons.

Workaround: Resolve the fragmentation cause. A possible solution is configuring TCP MSS on the following interface:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ft_admss.html

- CSCtq91063

Symptoms: A Cisco router may unexpectedly reload due to bus error or generate a spurious access.

Conditions: This symptom occurs when fragmentation of a tunneled packet fails due to the F/S particle pool running out of free particles. The F/S pool is used for fragmentation, so exhaustion of this pool will occur when there is a large amount of traffic flowing for which fragmentation is required. By default, path MTU discovery is enabled for tunnels which means that fragmentation is done at the tunnel interface, rather than the underlying interface and this issue is not hit. If the MTU is overridden, then it may become exposed to this issue. Assuming the tunnel is over an Ethernet interface with MTU of 1500, this will happen by setting the tunnel MTU to greater than 1476 bytes.

Workaround 1: Remove MTU override from the tunnel interface.

Workaround 2: Configure “service disable-ip-fast-frag”.

Workaround 3: Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- CSCtr79748

Symptoms: Memory leak occurs with the “ip tcp header-compression” configuration on the Virtual-Template interface.

Conditions: This symptom is observed when “ip tcp header-compression” is configured on the Virtual-Template interface.

Workaround: Delete “ip tcp header-compression”.

- CSCts65564

Symptoms: In a large-scale DMVPN environment, a DMVPN hub router may crash in the Cisco IOS process under high-scale conditions.

Conditions: This symptom only occurs if CRL caching is disabled (with the **crl cache none** command under the pki trustpoint configuration).

Workaround: Enable CRL caching (this is the configured default).

- CSCtt40285

Symptoms: The router crashes. The following message is displayed:

```
System returned to ROM by bus error at PC 0x629D2EBC, address 0xB0D0B11 at
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x629D2EBC
```

Conditions: This symptom is observed across multiple Cisco IOS Releases such as Cisco IOS Release 15.1(4)M2 and Cisco IOS Release 15.2(4)M1. This issue occurs only if NAT SIP ALG processing is enabled on the router.

Workaround: This crash can be prevented by disabling NAT SIP ALG processing on the router by issuing the **no ip nat service sip** command.

- CSCtu08373

Symptoms: The router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.

Conditions: This symptom occurs when the Cisco IOS firewall is configured and traffic flows through the router.

Workaround: There is no workaround.

- CSCtu23195

Symptoms: The SNMP ifIndex for serial interfaces (PA-4T/8T) becomes inactive after PA OIR.

Conditions: This symptom is observed with a PA OIR.

Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtw79510
Symptoms: VPN client users cannot be forced to change their passwords in the next login.
Conditions: This symptom is observed with an authentication problem while using the password change option.
Workaround: There is no workaround.
- CSCtw89123
Symptoms: A router may crash after configuring “ppp fragment delay”.
Conditions: This symptom is observed when “ppp fragment delay” + policy-map is configured on a multilink interface and traffic crosses the device.
Workaround: Increase “ppp multilink fragment delay” under a multilink interface.
- CSCtx56174
Symptoms: A Cisco router hangs until a manual power cycle is done. If the **scheduler isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.
Conditions: This symptom is seen with websense URL filtering enabled and with zone based firewalls.
Workaround: Disable URL-based filtering.
- CSCtx86539
Symptoms: NAT breaks SIP communication with addition of media attributes.
Conditions: This symptom is observed with NAT of SIP packets.
Workaround: There is no workaround.
- CSCty51453
Symptoms: Certificate validation using OCSP may fail, with OCSP server returning an “HTTP 400 - Bad Request” error.
Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T2 and later releases.
Workaround 1: Add the following commands to change the TCP segmentation on the router:

```
router(config)# ip tcp mss 1400
router(config)# ip tcp path-mtu-discovery
```


Workaround 2: Use a different validation method (CRL) when possible.
- CSCty56850
Symptoms: Routers are not updating the cnpdAllStatsTable with traffic from all expected protocols.
Conditions: This symptom is observed with routers that are running Cisco IOS 15.x (tested in 15.0, 15.1, and 15.2(2)T).
Workaround 1: Use the following CLI to get the stats for all the protocols:
show IP NBAR protocol-discovery
Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.
- CSCty61216
Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.
Conditions: This symptom is observed with the following IOS image:
c5350-jk9su2_ivs-mz.151-4.M2.bin.

It is seen with an outgoing SIP call from the gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

Workaround: There is no workaround.

- CSCty91465

Symptoms: Ping to a global IP address (interface not part of any VRF) received via a VRF interface does not work even when “vrf receive” and the policy maps are configured correctly to receive the packets from the VRF interface.

Conditions: This symptom is observed when CEF is enabled.

Workaround: Disable CEF.

- CSCtz22112

Symptoms: A VXML gateway may crash while parsing through an HTTP packet that contains the “HttpOnly” field:

```
//324809//HTTTPC:/httpc_cookie_parse: * cookie_tag=' HttpOnly'
//324809//HTTTPC:/httpc_cookie_parse: ignore unknown attribute: HttpOnly
```

```
Unexpected exception to CPU: vector D, PC = 0x41357F8
```

Note: The above log was captured with “debug http client all” enabled to generate additional debugging output relevant to HTTP packet handling.

Conditions: This symptom is observed when an HTTP packet with the “HttpOnly” field set is received.

Workaround: There is no workaround.

- CSCtz23020

Symptoms: The EZVPN client running a Cisco IOS Release 15.x code shows a corrupted ISAKMP lifetime value due to which the rekey is not triggered and can cause an outage.

Conditions: This symptom is observed when IKE uses certificate-based authentication.

Workaround: Use pre-shared keys.

- CSCtz33622

Symptoms: Multiple crashes on a Cisco ISR that is running latest IOS versions with x25 encapsulation due to managed timer corruption.

Conditions: This symptom is observed on a Cisco ISR using x25 routing.

Workaround: There is no workaround.

- CSCtz35999

The Cisco IOS Software Protocol Translation (PT) feature contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-pt>

- CSCtz40460

Symptoms: A router running Cisco IOS may crash or hang.

Conditions: This symptom may be seen when SSLVPN is configured with NTLM authentication. NTLM authentication is configured by default.

Workaround: There is no workaround.

- CSCtz47595

Symptoms: Dial string sends digits at incorrect times.

Conditions: This symptom is seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDm2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.

When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be 2 seconds, three commas = 3 seconds, and so on.

- With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, that is: 919195551212x,22 or 1212x,,,22.
- With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, that is: 919195551212x22.

Dialing directly to a number with no extension or extra digits works as expected.

Workaround: There is no workaround.

- CSCtz58941

Symptoms: The router crashes when users execute the **show ip route XXXX** command.

Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of “XXXX” networks are removed.

Workaround: The **show ip route XXXX** command (without “XXXX”) does not have the problem.

- CSCtz62766

Symptoms: One or more linecards may be reset. Persistent in the logs:

```
%SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
(608/2),process = CEF LC Stats.
```

until:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CEF LC Stats.
```

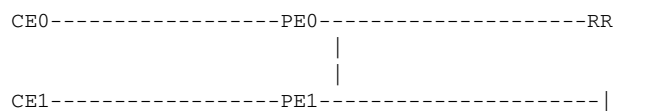
Conditions: This symptom can be seen on distributed platforms running Cisco IOS Release 12.4T or a later code.

Workaround: Use Cisco IOS 12.4 mainline code, such as Cisco IOS Release 12.4(25f), which is not susceptible.

- CSCtz71084

Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:



Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix:

no network x.x.x.x mask y.y.y.y

Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external.

Workaround: Hard clear.

- CSCtz78943

Symptoms: A Cisco router experiences a spurious access or a crash. Cisco ISR-G1 routers such as 1800/2800/3800 experience a spurious access. Cisco ISR-G2 routers such as the Cisco 2900/3900 routers that use a Power PC processor crash because they do not handle spurious accesses.

Conditions: This symptom occurs after enabling a crypto map on an HSRP-enabled interface. The exact conditions are being investigated.

Workaround: There is no workaround.

Further Problem Description: The CSCtx90408 DDTS was originally filed to fix this issue. Unfortunately, this caused another issue, which was addressed by backing out of the changes. The fix was backed out in the CSCty83376 DDTS, so this DDTS (CSCtz78943) will address both issues.

- CSCtz89334

Symptoms: A traffic blackhole is seen while a single pair of 4-wire EFM bond connections is down on a Cisco 888E router.

Conditions: This symptom occurs when connecting to an Ericsson DSLAM from a Cisco 888E router.

Workaround: There is no workaround.

- CSCua12317

Symptoms: The Cisco 3900 router resets when configuring Object Group/ACL when there is traffic on the interface where an ACL match is needed.

Conditions: This symptom is observed with the following conditions:

- The ACL definition should have service OG ACE.
- Reconfigure the service OG ACE or delete it.
- Traffic should be passing on the interface where the OG is applied when the above operation is performed.

Workaround 1: Configure a new ACL with the changes needed and apply it to the interface of interest, instead of modifying the already applied one. This is recommended when a configuration change is needed.

Workaround 2: Remove ACL checks on the interface when changing the configuration (“no ip access-group”).

- CSCua12945

Symptoms: Applying QoS under the serial interface is causing the interface to flap and most of the time causes line protocol to be DOWN.

Conditions: This symptom occurs during both congestion and non-congestion on the link.

Workaround: Doing a shut/no shut on the interface makes the interface come UP and running.

- CSCua15003

Symptoms: When a call is canceled mid-call, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

Conditions: This symptom can occur in the following situations:

- CUBE receives 180 ringing with SDP session.
- “media transcoder high-density” is enabled.

Workaround: Disable “media transcoder high-density”.

- CSCua19294

Symptoms: IPSLA intermittently reports wrong minimum RTT of 1 millisecond or below.

Conditions: This symptom is observed on microsecond precision setting sending multiple number-packets at 100msec intervals.

Workaround: There is no workaround.

- CSCua24689

Symptoms: Fragments are sent without label resulting in packet drops on the other side.

Conditions: This symptom is observed under the following conditions:

- MPLS enabled DMVPN tunnel on egress.
- VFR on ingress.

Workaround: Disable VFR if possible.

- CSCua39390

Symptoms: The PRI configuration (voice port) is removed after a reload:

```
interface Serial1/0:23      ^
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
      ^
% Invalid input detected at '^' marker.
isdn incoming-voice voice
      ^
% Invalid input detected at '^' marker.
no cdp enable
      ^
% Invalid input detected at '^' marker.
voice-port 1/0:23
      ^
% Invalid input detected at '^' marker.
```

Also, the following traceback is seen:

```
%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T and Cisco IOS Release 15.1(4)M4 after reload. The issue does not occur in Cisco IOS Release 12.4(24)T6 or earlier releases.

Workaround: Reapply the configuration after the router comes back up.

- CSCua40273

Symptoms: The Cisco ASR 1000 router crashes when displaying MPLS VPN MIB information.

Conditions: This symptom occurs on the the Cisco ASR 1000 with Cisco IOS Release 15.1(02)S software.

Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua50697

Symptoms: After unplugging and reconnecting a T1 cable, the T1 controller remains down or reports continuous errors. After a router reload, the T1 controller remains up until the cable is disconnected again.

Conditions: This symptom affects only the following cards:

- HWIC-xCE1T1-PRI
- NM-8CE1T1-PRI
- VWIC3-xMFT-T1/E1
- GRWIC-xCE1T1-PRI

The T1 signal must also be out-of-specification according to T1.403 standards.

Workaround 1: Reload the router with the T1 cable plugged in.

Workaround 2:

1. Upgrade to a fixed-in Cisco IOS version.
2. Issue the following commands (hidden, so tab complete will not work):

```
enable
config t
controller <t1/e1> <slot/subslot/port> ! ( example: controller t1 0/0/0 )
hwic_t1e1 equalize
```

3. Shut/no shut the T1 controller, or reload the router to allow the CLI to take effect.

- CSCua55629

Symptoms: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

Conditions: The **show memory debug leaks** command shows a CCSIP_SPI_CONTORL leak with size of 6128 and points to the event “SIPSPI_EV_CC_MEDIA_EVENT”:

Adding blocks for GD...

```

                                I/O memory

Address      Size  Alloc_pc  PID  Alloc-Proc      Name
-----
                                Processor memory

Address      Size  Alloc_pc  PID  Alloc-Proc      Name
286E144 6128  8091528  398  CCSIP_SPI_CONTR  CCSIP_SPI_CONTROL
```

Workaround: There is no workaround.

- CSCua55785

Symptoms: Build breakage due to the fix of CSCtx34823.

Conditions: This symptom occurs with the CSCtx34823 fix.

Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua55797

Symptoms: The **privilege exec level 0 show glbp brief** command causes the memory to be depleted when the **show running** or **copy running-config startup-config** commands are used. The configurations will then show this:

```
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief
privilege exec level 0 show glbp
privilege exec level 0 show
```

Removing the configurations causes this to happen over and over until the Telnet session is terminated:

```
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
```

If the configurations are saved and the device is reloaded, the device will not fully boot until the configurations are bypassed.

Conditions: This symptom occurs after the **privilege exec level 0 show glbp brief** command is entered and saved.

Workaround: Reload the router before saving the configurations.

- CSCua61201

Symptoms: Unexpected reload with BFD configured.

Conditions: This symptom occurs when a device is configured with BFD.

Workaround: There is no workaround.

- CSCua61330

Symptoms: Traffic loss is observed during switchover if,

1. BGP graceful restart is enabled.
2. The next-hop is learned by BGP.

Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

Workaround: There is no workaround.

- CSCua82425

Symptoms: A Cisco router may unexpectedly reload when using EMM when choosing a menu option that executes “reload” or “do reload”.

Conditions: This symptom occurs if there are unchanged configuration changes.

Workaround: Change the menu option to save the configuration before the reload. If you do not want to save the configuration, then there is no currently known workaround.

Further Description: In the newer code, the crash does not occur with “do reload” (though “reload” still crashes), but it still does not result in the desired behavior or reloading the device.

- CSCua91698

Symptoms: ephone-type disappears from the running-configuration.

Conditions: This symptom occurs in SRST mode and after reload.

Workaround: Reconfigure the ephone-type commands and again save to the startup-configuration.

- CSCua99969

Symptoms: IPv6 PIM null-register is not sent in the VRF context.

Conditions: This symptom occurs in the VRF context.

Workaround: There is no workaround.

- CSCub13317

Symptoms: The Cisco 2900 with VWIC2-2MFT-T1/E1 in TDM/HDLC mode does not forward any traffic across the serial interface after a certain amount of time.

Conditions: This symptom occurs when you configure frame relay over VWIC2 channel-group in TDM/HDLC mode.

Workaround: Configure VWIC2 channel-group in NMSI mode.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C>

CVE ID CVE-2012-3918 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub18682

Symptoms: The phone number is missing in the Sent INVITE from CUBE when testing OutBound Dial-Peer Matching using the phone number and context under destination-uri.

Conditions: This symptom occurs when running Cisco IOS Release 15.2(2)T1.12.

Workaround: There is no workaround.

- CSCub19185

Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

Workaround: There is no workaround.

- CSCub41748

Symptoms: The router displays high CPU usage due to NBAR.

Conditions: This symptom occurs due to RTP traffic.

Workaround: Replace “protocol rtp” with ACL in match statement.

- CSCub45303

Symptoms: H323 to SIP interworking calls fail.

Conditions: This symptom is observed with the following topology:

```
callgen----ogw-----cube1-----cube2-----tgw----callgen
```

The following call combinations fail:

HHHS,HSSH,SHHS,HSSS.

Workaround:

1. Configure voice CLIs on the router.
2. Save the configurations.
3. Reload the router and rerun the calls.

- CSCub55790

The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

Affected devices that are configured as Smart Install clients are vulnerable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall>

- CSCub61009

Symptoms: Spurious errors are observed on the Cisco AS5400.

Conditions: This symptom is observed on the Cisco AS5400.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C>

CVE ID CVE-2012-5422 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub61795

Symptoms: The log fills with SYS-2-BADSHARE messages, leading to a crash.

```
%SYS-2-BADSHARE: Bad refcount in retparticle, ptr=69AD4440, count=0
-Traceback= 601E887Cz 601E50B4z 601E56C0z 602D24CCz 60F38F04z 6065B628z
Invalid magic number in receive buffer (0x0)
```

Conditions: This symptom occurs with a large amount of traffic passing through an ATM interface. This issue might be specific to an ATM interface using the CX27470 ATMOC3 driver as seen in the **show interface** command output. The ATM module that the issue was originally seen on was a NM-1A-OC3-POM. QOS might be needed to trigger the issue.

Workaround: A possible but unconfirmed workaround is to disable QOS on the interface.

- CSCub70336
 Symptoms: The router can crash when “clear ip bgp *” is done in a large-scale scenario.
 Conditions: This symptom is observed only in a large-scale scenario, with ten of thousands of peers and several VPNv4/v6 prefixes.
 Workaround: “clear ip bgp *” is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.
- CSCub80491
 Symptoms: A Cisco router may experience alignment errors. These alignment errors may then cause high CPU.
 Conditions: This symptom occurs as the alignment errors require using Get VPN. It is currently believed to be related to having the Get VPN running on a multilink interface, but this is not yet confirmed.
 Workaround: There is no workaround.
- CSCub86011
 Symptoms: The embedded event manager (EEM) is not available on the Cisco VG202/204.
 Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T or later releases.
 Workaround: There is no workaround.
- CSCub86706
 Symptoms: After multiple RP switchover, the router crashes with the “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO” error.
 Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.
 Workaround: There is no workaround.
- CSCub91111
 Symptoms: Outgoing packet drop on the HSPA+R7 cellular interface with SWI MC8705 firmware T3.5.x (not released).
 Conditions: This symptom is observed on HSPA+R7 SKU with MC8705 T3.5 firmware (not released firmware).
 Workaround: Use MC8705 firmware T1.x release.
- CSCub91815
 Symptoms: Certificate validation fails with a valid certificate.
 Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.
 Workaround: There is no known workaround.
- CSCub98623
 Symptoms: The **show int** command output displays the input queue size as bigger the 0, and never goes down. Shut/no shut does not help as well.
 Conditions: This symptom is observed with the following conditions:
 - A Cisco IOS router actions as XOT.

- The XOT Server becomes not reachable for sometime while the x25 client is attempting to send traffic.
- Cisco IOS Release 12.4(24)T7, Cisco IOS Release 15.1M, or later releases.

Workaround: Increase the input hold queue size from default 75 to max. Monitor it periodically manually or by script and perform a planed reload when the queue size is close to max.

- CSCuc07984

Symptoms: The Cisco 819 router serial interface does not interoperate with modems such as Adtran, Aethra, and Pardayn.

Conditions: This symptom occurs on the serial interface on the Cisco 819 series router while connecting to some specific types of modems.

Workaround: There is no workaround.

- CSCuc12685

Symptoms: Address Error exception is observed with ccTDUtilValidateDataInstance.

Conditions: This symptom is observed with ccTDUtilValidateDataInstance.

Workaround: There is no workaround.

- CSCuc16172

Symptoms: When the reset button is pushed on a Cisco C881W-A-K9 router, the start-up configuration is automatically backed up as “startup.backup.xxx” and stored in the flash.

Conditions: This symptom occurs when an xxx.cfg file is present on the flash and the push button is pressed. The Cisco C881W-A-K9 Router boots up with the xxx.cfg file present on the flash, but also backs up the start-up configuration as “startup.backup.xxx” and stores it on the flash.

Workaround: There is no workaround.

- CSCuc19862

Symptoms: Traceback and CPU hog is seen due to spurious memory access when Flexible NetFlow (FNF) is enabled.

Conditions: This symptom is seen when enabling Flexible NetFlow.

Workaround: Use classic NetFlow or configure FNF on the tunnel template interface (preferred).

- CSCuc37365

Symptoms: The **bandwidth** command under the cellular interface goes back to the default bandwidth of 50K after a reload or modem reset/power-cycle.

Conditions: This symptom is observed when you configure the **bandwidth** command.

Workaround: There is no workaround.

- CSCuc38253

Symptoms: The Cisco C3900 router crashes due to “Unexpected exception to CPU: vector 1400”.

Conditions: The exact conditions are still being investigated.

Workaround: There is no workaround.

- CSCuc39963

Symptoms: Spurious memory access/crash is seen at mdb_tree_classify.

Conditions: This symptom occurs when the egress QoS policy is configured.

Workaround: There is no workaround.

- CSCuc42518

Symptoms: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that allows a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition while trying to process certain RTCP packets during media negotiation using SIP.

Conditions: This symptom occurs when Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when a certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.

Workaround: Increase the interface input queue size. Disable Video if not necessary.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C>

CVE ID CVE-2012-5427 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc42558

Symptoms: A Cisco router configured as the VXML gateway may experience a leak in the processor memory pool in CCSIP_SPI_CONTROL in the function url_parseTelUrl.

Conditions: This symptom occurs when a Cisco router is configured as the VXML gateway. There could be other triggers as well.

Workaround: Reload the router during a maintenance window to avoid an unexpected crash. You may also downgrade to Cisco IOS Release 15.1(4)M3, which is not affected.

- CSCuc47675

Symptoms: Traffic blackhole when a single pair of 4-wire EFM bond connection is down on a Cisco 888E router.

Conditions: This symptom is observed when connecting to a third-party vendor DSLAM from a Cisco 888E router.

Workaround: There is no workaround.

- CSCuc56259

Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

```
%VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times
```

and

```
Delivery Ack could not be sent due to lack of buffers.
```

Conditions: This symptom occurs when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc59541

Symptoms: Spoke fails to learn networks behind other spokes and EIGRP flapping occurs.

Conditions: This symptom is observed with a FlexVPN spoke-to-spoke setup.

Workaround: There is no workaround.

- CSCuc63884

Symptoms: A router configured with HSRP and RF interdev may experience an NMI watchdog during reload after failover, as it transitions from a standby to an active state.

```
SYS-2-INTSCHED 'sleep for' at level 6 -Process= "RF Interdev reload process", ipl= 6,
pid= 316
NMI Watchdog timeout!:: vector 2, PC = 0x219B3C
```

Conditions: This symptom is observed with HSRP and interdev configured. HSRP failover is triggered by link failure if the configuration is being saved at the same time.

Workaround: There is no workaround.

- CSCuc70472

Symptoms: Compression (V.42bis, V.44) is disabled by “modemcap” for PVDm2-DM. After some time, certain modems start to negotiate V.44/V.42bis and drop those calls before PPP. The number of modems negotiating compression is growing over time, leading to an increase in the drop call rate.

Conditions: This symptom occurs when the following modemcap is applied:

```
"modemcap entry V32bis_noComp1:MSC=&F0+DCS=0,0;+MS=10,0,4800,14400" OR
"modemcap entry V32bis_noComp2:MSC=+MS=10,0,4800,14400;%C0"
```

Breakdown:

```
"+DCS=0,0=0,0" - V.44 OFF, V.42bis OFF
"+MS=10,0,4800,14400" - V.32bis, No V8.bis, min 4800, max 14400
"%C0" - No compression
```

After reload:

```
Router#sh modem log 0/463 | i compression
Data compression          69      None
Data compression          69      None
Data compression          69      None
Data compression          69      None << No compression
Router#sh modem configuration 0/463 | i S41|S82
S41 = 137      Compression selection is MNP 5 Retrain and fallback/fall
forward disabled
S82 = 128      Break Handling Options/LAPM Break Control = 0x80
S82 = 21
```

A few hours/days after reload:

```
Router#sh modem log 0/463 | i compression
Data compression          68      None
Data compression          68      V44 << Starts to negotiate V.44, even
while disabled by modemcap
Data compression          68      V44
Data compression          68      V44
Router#sh modem configuration 0/463 | i S41|S82
S41 = 139      Compression selection is MNP 5 and V.42 bis
S82 = 128      Break Handling Options/LAPM Break Control = 0x80
S82 = 25
```

Workaround: Reload.

- CSCuc79143

Symptoms: The cellular driver should handle the profile getting inactive and should bring down the cellular interface.

- Conditions: This symptom occurs when the profile is deactivated by the HA.
- Workaround: Doing a “clear line” will bring down the cellular interface and restore the connection.
- CSCuc91717

Symptoms: The router crashes when making a basic x25 configuration change.

Conditions: This symptom occurs when you remove the x25 translation statement from the running configuration when traffic is on.

Workaround: Shut the interface before making the x25 configuration change.
 - CSCud01502

Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

Conditions: This symptom occurs in CME.

Workaround: There is no workaround.
 - CSCud05636

Symptoms: The MAC-address gets corrupted when a user sends the multicast traffic.

Conditions: This symptom is observed with the Cisco IOS Release 15.1(4)M3 image, whereas the same multicast traffic works as expected with the Cisco IOS Release 12.4T image.

Workaround: A possible workaround is to enable the **ip pim nbma- mode** command at the CPE end.
 - CSCud06180

Symptoms: When the SDK crash occurs, the cellular interface is not operational.

Conditions: This symptom occurs when the IPSLA is present on the cellular interface, and you power-cycle the modem 8-10 times, causing the CWAN_SHIM layer to crash.

Workaround: There is no workaround.
 - CSCud22148

Symptoms: The E1 (E&M) controller is down.

Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M2 or later releases. This issue is seen with the Cisco 3945.

Workaround: There is no workaround.
 - CSCud33159

Symptoms: Excessive loss of MPLS VPN traffic and high CPU utilization is observed due to the process switching of MPLS traffic over the ATM interface.

Conditions: This symptom occurs when MPLS is enabled on the ATM interface with aal5snap encapsulation.

Workaround: There is no workaround.
 - CSCud46314

Symptoms: The Cisco router crashes when polling ciscoEnvMonSupplyStatusDescr MIB.

Conditions: This symptom is observed when the ciscoEnvMonSupplyStatusDescr MIB is getting polled.

Workaround: Apply the following to block the view:

 - snmp-server view blockmib iso include
 - snmp-server view blockmib 1.3.6.1.4.1.9.9.13.1.5.1.2 exclude

Similarly, apply the following to the community:

- snmp-server community <community> view blockmib ro
- CSCud46826

Symptoms: The Cisco 7200 VSA may stop encrypting outbound traffic for some SAs in a dual-Hub Phase 3 DMVPN setup. Inbound traffic is decrypted correctly by the Cisco 7200 Hub. Only outbound traffic is affected. The following error can sometimes be seen:

```
Dec 1 2012 18:24:39.261 MSK: %VPN_HW-1-PACKET_ERROR: slot: 0 Packet
Encryption/Decryption error, Invalid
SA:srcadr=192.168.200.5,dstadr=192.168.200.11,size=88
```

This error causes EIGRP flapping on the Hub due to unidirectional connectivity. For example:

```
Dec 1 2012 18:11:43.779 MSK: %DUAL-5-NBRCHANGE: EIGRP-IPv4 77: Neighbor 192.168.20.20
(Tunnell) is down: retry limit exceeded
Dec 1 2012 18:11:46.107 MSK: %DUAL-5-NBRCHANGE: EIGRP-IPv4 77: Neighbor 192.168.20.20
(Tunnell) is up: new adjacency
```

EIGRP may come up on a spoke, but it eventually goes down with:

```
Dec 1 2012 18:10:23.317 MSK: %DUAL-5-NBRCHANGE: EIGRP-IPv4 77: Neighbor 192.168.20.3
(Tunnell) is down: holding time expired
```

Conditions: This symptom is observed with Cisco 7200. The issue is not seen with software crypto engine. The issue is not seen on the Cisco ASR 1000 Hub with Cisco IOS Release 15.2(4)S1 and the same configuration. The issue is not seen in a test setup if a single Spoke is connected.

The issue with one IPsec SA can be resolved by clearing this SA, but it may affect another SA that was working before. It was noticed that first Phase 2 rekey may resolve the issue completely.

To diagnose this issue, check if the “pkts encaps” counter is incremented:

```
BSNS-7200-1#show crypto ipsec sa peer 192.168.200.10 | i ident|caps
  local ident (addr/mask/prot/port): (192.168.200.5/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (192.168.200.10/255.255.255.255/47/0)
    #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
    #pkts decaps: 130, #pkts decrypt: 130, #pkts verify: 130
BSNS-7200-1#show crypto ipsec sa peer 192.168.200.10 | i ident|caps
  local ident (addr/mask/prot/port): (192.168.200.5/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (192.168.200.10/255.255.255.255/47/0)
    #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
    #pkts decaps: 132, #pkts decrypt: 132, #pkts verify: 132
```

Workaround: This issue is not seen in Cisco IOS Release 15.1(4)M3a. Cisco IOS Release 15.1(4)M5 is known to be affected.

- CSCud86954

Symptoms: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn’t get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

The following is sample output when all cache entries are lost:

```
Router#sh flow monitor FNF-MON stat
  Cache type:                               Normal
  Cache size:                               4096
  Current entries:                           0
  High Watermark:                           882
  Flows added:                               15969
  Flows not added:                           32668
```

```

Flows aged:
- Active timeout      (1800 secs)      0
- Inactive timeout    (15 secs)      15969
- Event aged          0
- Watermark aged      0
- Emergency aged      0

```

Conditions: This symptom occurs when all of the following are true:

- Flexible Netflow is enabled on a DMVPN tunnel interface.
- Local policy-based routing is also enabled on the router.
- Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

Workaround: Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.

Resolved Caveats—Cisco IOS Release 15.1(4)M5

Cisco IOS Release 15.1(4)M5 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M5 but may be open in previous Cisco IOS releases.

- CSCsg36725

Symptoms: A memory leak and memory exhaustion may occur when QoS policies are updated on 40,000 sessions.

Conditions: This symptom is observed on a Cisco 10000 series router, but may also affect other platforms.

Workaround: There is no workaround.

- CSCth20872

Symptoms: The following error message is seen accompanied by a reset of the Fast Ethernet:

```
%C870_FE-3-TXERR: FastEthernet0: Fatal transmit error. Restarting...
```

Conditions: This symptom is observed on a Cisco 877 router that is running Cisco OS Release 12.4(24)T3.

Workaround: There is no workaround.

- CSCth43911

Symptoms: The system may crash when performing the SNMP SET operation for CISCO-CALLHOME-MIB objects in callHomeDestEmailAddressTable, ccmSeverityAlertGroupTable, ccmPeriodicAlertGroupTable, ccmPatternAlertGroupTable, ccmEventAlertGroupTable, and ccmDestProfileTestTable.

Conditions: This symptom does not occur under any specific conditions.

Workaround: There is no workaround. The fix exists in Cisco IOS Release 12.2(33)SXJ and Cisco IOS Release 12.2(50)SY.

- CSCth56654

Symptoms: When making calls in a CVP solution environment, the call is not established.

Conditions: This symptom is observed when CUBE is enabled with the “connection-reuse” CLI, which supersedes handling of the VIA header for SIP response messages.

Workaround: Disable the “connection-reuse” CLI.

- CSCth92828
Symptoms: When viewing a device configuration, such as via a URL like https://tools.cisco.com/sch/reports/viewDeviceConfiguration.do?specific_item_query, the TACACS server key, a type 7 reversible password, is still visible.
Conditions: This symptom is observed when viewing a device configuration.
Workaround: There is no workaround.
- CSCti87194
Symptoms: The last fragment causes a crash because of an invalid zone value.
Conditions: This symptom occurs when a Big IPC message is fragmented. Then, the last fragment causes the crash because of an invalid zone value.
Workaround: There is no workaround.
- CSCtj10515
Symptoms: A crash is seen in the IGMP input process.
Conditions: This symptom is observed in a multi-VRF scenario with extranet MVPN.
Workaround: There is no workaround.
- CSCtj14921
Symptoms: Memory leak is seen in the crypto SS process.
Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M2.
Workaround: If possible, reload the router periodically.
- CSCtj48387
Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP-related errors.
Conditions: This symptom occurs when DHCP is enabled and sessions get DHCP information from a RADIUS server.
Workaround: There is no workaround.
Further Problem Description: This fix needs to be included in the Cisco ME 3400.
- CSCtj59117
Symptoms: The following error message is seen and the router freezes and crashes:

```
%SYS-2-BADSHARE: Bad refcount in retparticle
```


A reload is required to recover.
Conditions: This symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Cisco IOS Release 12.4(15)T14.
Workaround: Remove CEF.
- CSCtl73132
Symptoms: The router may crash and reset when the **show ipc hog-info** command or the **show tech-support ipc** command is run repetitively on either the switch processor or route processor.
Conditions: The issue can be seen when the **show ipc hog-info** command or the **show tech-support ipc** command is run repetitively on either the switch processor or route processor.
Workaround: Do not use the **show ipc hog-info** command or the **show tech-support ipc** command.

- CSCtn55070

Symptoms: Call-home http messages can hang and not be sent out.

Conditions: This symptom is observed when call home is enabled and an http transport method is used. This symptom is timing-dependent and cannot be hit every time. In addition, this symptom is observed in telnet sessions.

Workaround: Log in to the console port if a telnet session was used to send call-home http messages. Because the console is waiting on user-supplied information (--More--), enter something into the console; the call-home process can then continue to execute.

- CSCto09059

Symptoms: CPUHOG at IPC Check Queue Time Process results in IOSD crash.

Conditions: This symptom occurs with multiple RP switchovers with ISG PPPoE sessions.

Workaround: There is no workaround.

- CSCto71671

Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

Workaround: There is no workaround.

- CSCtq21258

Symptoms: When a user uses a password larger than 32 bytes in size, the authentication for COA will pass if the password matches the settings on the RADIUS server. When this password is reduced in size to exactly 32 bytes, including the setting on the RADIUS server, the authentication for the COA will fail as the ISG appends excess data to the password sent to the RADIUS for authentication.

Conditions: This symptom is seen when the user password is larger than 32 bytes and is being reduced to exactly 32 bytes.

Workaround: Do not use 32 bytes as the size for the user password. In case the error occurs, the only method to solve the issue is to reload the device.

- CSCtr87070

Symptoms: Enable login fails with the error “% Error in authentication”.

Conditions: This symptom is observed with TACACS single-connection.

Workaround: Remove TACACS single-connection.

- CSCts03251

Symptoms: A Cisco 2921 router running Cisco IOS Release 15.1(4)M with the “logging persistent” feature configured may crash.

Conditions: This symptom is observed with the “logging persistent” feature.

Workaround: Disable the “logging persistent” feature.

- CSCts32708

Symptoms: Similar to CSCth80642, the Cisco IOS SSLVPN router fails to accept new sessions. Users will not be able to load the WebVPN login page. If debug sdps is enabled, the following error message may be displayed:

Sev 4:sdps_get_pak_from_tcp(),line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC
 Conditions: This symptom occurs when the router remains reachable; otherwise, (that is, you can ping the WebVPN IP) the SSL process is running and listening on the right port. The **show tcp tcb** and **show tcp brief all numeric** command output will show connections stuck in CLOSED and CLOSEWAIT state. Clearing the TCP TCB sessions does not restore connectivity. Taking WebVPN in/out of service does not restore connectivity. Disabling WebVPN CEF and rebooting does not prevent the issue. Rebooting does resolve the issue temporarily.

Workaround:

1. Reboot.
2. If available for your platform, get the fix for CSCth80642 and disable webvpn cef (you should reboot or clear the tcb connections after disabling WebVPN CEF). This may prevent the problem.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: \CVE ID CVE-2011-3286 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts33018

Symptoms: The Cisco UC500 crashes at Dot11 subsystem after being upgraded from SWP 8.1.0 (15.1(2)T2) to SWP 8.2.0 (15.1(2)T4)

Conditions: This symptom is observed when a Cisco 2900 PoE switch is connected to the Cisco UC540 with Cisco phones and an iMac is connected to the switch. An Apple laptop is also connected using wireless.

Workaround: There is no workaround.

- CSCts56044

Symptoms: A Cisco router crashes while executing a complex command. For example:

```
show flow monitor access_v4_in cache aggregate
ipv4 precedence sort highest ipv4 precedence top 1000
```

Conditions: This symptom is observed while executing the **show flow monitor top** top-talkers command.

Workaround: Do not execute complex flow monitor top-talkers commands.

- CSCts68626

Symptoms: PPPoE discovery packets causes packet drop.

Conditions: This symptom is observed when you bring up a PPPoE session and then clear the session.

Workaround: There is no workaround.

- CSCts69204

Symptoms: PPPoE sessions do not get recreated on the standby RP.

Conditions: This symptom occurs on the standby RP.

Workaround: There is no workaround.

- CSCts72911

Symptoms: In case of a GR/NSF peering, after an SSO, the restarting router (PE, in this case) does not advertise RT constrain filters to the nonrestarting peer (RR, in this case).

Conditions: This symptom is observed after an SSO in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

Workaround: There is no workaround.

- CSCts87612

Symptoms: Traffic over L2TPv3 becomes very slow. Ping shows high latency.

Conditions: This symptom is observed when EHWIC-1GE-SFP-CU is used as the xconnect interface.

Workaround: Do shut/no shut on the EHWIC-1GE-SFP-CU interface

- CSCtt26208

Symptoms: A Cisco 3845 running Cisco IOS Release 15.1(4)M1 may have a processor pool memory leak in CCSIP_SPI_CONTROL.

Conditions: The conditions are not known at this time.

Workaround: There is no workaround.

- CSCtt26692

Symptoms: The router crashes due to memory corruption. In the crashinfo you may see:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxxx data xxxxxxxx
chunkmagic xxxxxxxx chunk_freemagic EF4321CD - Process= "CCSIP_SPI_CONTROL", ipl= 0,
pid= 374 chunk_diagnose, code = 1 chunk name is MallocLite
```

Conditions: This symptom occurs when the router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- CSCtt61762

Symptoms: IPv6 hosts connected to EHWIC-*ESG Layer 2 ports are not able to communicate to each other locally (at Layer 2).

Conditions: This symptom was first noticed on a Cisco ISR G2 with EHWIC-*ESG and directly connected IPv6.

Workaround: There is no workaround.

- CSCtv36812

Symptoms: Incorrect crashInfo file name is displayed during crash.

Conditions: This symptom is observed whenever a crash occurs.

Workaround: There is no workaround.

- CSCtw45480

Symptoms: Inbound GRE encapsulated traffic is dropped with the “Unknown-l4 sessions drop log” message on the router with ZBFW.

Conditions: This symptom is observed when router self zone policies are applied and the GRE tunnel is in an intermediate zone between the inside and outside zones.

Workaround: Remove the self zone policies.

- CSCtw46229
Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.
Conditions: This symptom is observed with PPP negotiations and the session involving PPPoA.
Workaround: Ensure all your PPP connections stay stable.
- CSCtw61872
Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.
Conditions: This symptom is observed when executing a complex sort with top-talkers on a **show** command from multiple CLI sessions (note that normal **show** commands without top-talkers are fine):

```
sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
```


Workaround: Do not execute complex sorts with top-talkers on the **show** output from multiple CLI sessions.
- CSCtw87132
Symptoms: A Cisco router may crash when clearing a TCP session:

```
router120#clear tcp tcb 08C5F4F8 [confirm]
SIGBUS (0xFF1BD460) : Bus Error ( [0xD0D0D39] invalid address alignment)
```


Conditions: This has been experienced on a Cisco 2921 router that is running Cisco IOS Release 15.1(4)M through to Cisco IOS Release 15.1(4)M3.
Workaround: There is no workaround.
- CSCtx06018
Symptoms: Interface queue wedge is seen when performing the WAAS performance test.
Conditions: This symptom is observed when performing the WAAS performance test.
Workaround: Increase the interface input queue hold size.
- CSCtx22322
Symptoms: If an over-temperature interrupt occurs when the CPU utilization is high, the system may crash.
Conditions: This symptom is observed when CPU utilization of the system is high in Cisco 880 series routers.
Workaround: There is no workaround.
- CSCtx32329
Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.
Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.
Workaround: Do not use static multicast routes, or make sure that the next-hop specified can always be resolved. Do not use the **show** command.
- CSCtx64684
Symptoms: While configuring the ISIS on two Cisco 2921 routers connected back to back, the ISIS neighbors do not come up.

Conditions: This symptom is observed only on the SVI interface. This issue is only seen with EHWIC.

Workaround: If the router has an L3 port, form a neighborship on a physical interface directly or create dot1q subinterfaces if peering is required on multiple VLANs.

- CSCtx66030

Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:

- SIP-CME
- SIP-SRST GW
- CUBE

Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.

Workaround: Limit the number of registrations/unregistrations to less than 320.

- CSCtx66804

Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

Conditions: This symptom is observed with the following conditions:

- “ppp lcp delay 0” is configured.
- Cisco IOS Release 15.0(1)M5.

Workaround: Set delay timer without 0.

- CSCtx71185

Symptoms: The router crashes due to corrupted program counter.

Conditions: This symptom is observed with packets being switched across the dialer interface.

Workaround: There is no workaround.

- CSCtx74342

Symptoms: After the interface goes down or is OIRed, in a routing table, you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next-hop interface set to the interface that is down.

Conditions: This symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

Workaround: Configuring SPF throttle timer can change the interval.

Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Router show ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       1 - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O      2001::/64 [110/10]
      via Ethernet0/0, directly connected
```

- CSCtx77750

Symptoms: Crosstalk may be heard by PSTN callers when a call is placed on hold and Music on Hold (MMOH) is enabled.

Conditions: CUCM is configured to do Multicast MoH.

Workaround:

(1) Disable H.323 Multicast MoH functionality in IOS or use SIP Multicast MoH. (2) Use Unicast MoH

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:ND/RC:C>

CVE ID CVE-2012-1361 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx85623

Symptoms: The ATM output queue is stuck, and the dialer loses the IP address. The following error messages are displayed:

```
Jul 5 10:16:45.430: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
Jul 5 10:16:45.442: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Jul 5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to down
Jul 5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed
state to down
Jul 5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed
state to down
```

```
Dialer Interface loses IP Address
n0920ar101#sh ip int brief
Interface          IP-Address      OK? Method Status
Protocol
Dialer1            unassigned     YES IPCP   up
up
```

```
Output Queue is Stuck at 40/40 and Drops increment at the VC Level
n0920ar101#sh queueing int atm0/3/0
Interface ATM0/3/0 VC 8/35
Queueing strategy: fifo
Output queue 40/40, 830 drops per VC << reaches 40/40 and drops increment at
the VC level
```

```
sn0920ar101#sh queueing int atm0/3/0
Interface ATM0/3/0 VC 8/35
Queueing strategy: fifo
Output queue 40/40, 833 drops per VC << reaches 40/40 and drops increment drops
increment at the VC level
```

Conditions: This symptom is observed with a Cisco ISR G1/G2 with HWIC-1ADSL Card, SRE/WAE. Crypto is enabled under the dialer interface, and CEF is also enabled. All these conditions are necessary to trigger the symptom.

Workaround 1: Reconfigure PVC(PVC reset will work only 23 times, after which reload is required).

Workaround 2: Disable the hardware crypto engine accelerator.

Workaround 3: Disable CEF.

Workaround 4: Reload the router.

- CSCtx92802

Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

Conditions: This symptom is observed under the following conditions:

- Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
- VRF enabled.
- CEF enabled.
- VPN tunnel.

Workaround: Disable VFR or CEF.

- CSCtx95840

Symptoms: A Cisco voice gateway may unexpectedly reload.

Conditions: This symptom is observed on a Cisco voice gateway running SIP protocol. In this case the issue was when sipSPIUfreeOneCCB() returns, the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

Workaround: There is no workaround.

- CSCty01234

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: This symptom is observed only with low-end platforms using VDSL interfaces, such as a Cisco 887 router. It also requires that the **qos pre-classify** command be used in conjunction with IPsec and GRE, such as in a DMVPN configuration.

Workaround: Do not use the **qos pre-classify** command.

- CSCty03745

Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

Conditions: This symptom occurs when the IPv4 default route exists, that is:

```
ip route 0.0.0.0 0.0.0.0 <next-hop>.
```

Or a certain static/IGP route exists: For example:

```
ip route 0.0.253.0 255.255.255.0 <next-hop>.
```

Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

```
router bgp 65000
 address-family l2vpn vpls
  neighbor 10.10.10.10 next-hop-self
```

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty04798

Symptoms: A Cisco router may experience a memory leak approximately 24 bytes in the dead process. The **show memory dead** output shows mostly the “show_voice_call_status_task” process.

Conditions: The following configuration is present:

```
pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 1
```

If nfas is not configured, there is no leak. This has been experienced on a Cisco 3825 router that is running Cisco IOS Release 12.4(15)T17 configured as a voice gateway.

Workaround: There is no workaround.

- CSCty05092

Symptoms: EIGRP advertises the connected route of an interface which is shut down.

Conditions: This symptom is observed under the following conditions:

1. Configure EIGRP on an interface.
2. Configure an IP address with a supernet mask on the above interface.
3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

Workaround 1: Remove and add INTERFACE VLAN xx.

Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty32232

Symptoms: BRI interface is not showing as monitored.

Conditions: This symptom occurs after performing an on-line insertion/removal of an NM-16ESW module.

Workaround: Reload the router.

- CSCty33945

Symptoms: When a SIP gateway tears down video and later sets it up again after a midcall invite for the same call, it reuses the same source RTP port as before. Unfortunately, it does not check if this RTP port is in use for a different call, and therefore crosstalk can occur.

```
4310820: Feb 27 17:56:08.910: //3017060/BF76175BB294/SIP/Media/sipSPIAddStream:  
Reusing old src_port(16384)
```

Conditions: This symptom is observed when a SIP gateway tears down video and later sets it up again after a midcall invite for the same call.

Workaround: There is no workaround.

- CSCty34020

Symptoms: A Cisco 7201 router's GigabitEthernet0/3 port may randomly stop forwarding traffic.

Conditions: This symptom only occurs on Gig0/3 and possibly Fa0/0 as both are based on different hardware separate from the first three built-in gig ports.

Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty42626

Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.

Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list)

```
c3925E, c3945E  
c2951, c3925, c3945
```

c7200/VAM2+/VSA,
possibly VPNSPA on c7600/cat6K
819H
ISR G2 routers with ISM IPsec VPN accelerator

Workaround: There is no workaround.

- CSCty43587

Symptoms: A crash is observed with memory corruption similar to the following:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
dealloc XXXXXXXX
```

Conditions: This symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

Workaround: There is no workaround.

- CSCty53243

Symptoms: Video call fails in the latest mcp_dev image

asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image

asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

Conditions: This symptom is observed when CUBE changes the video port to "0" in 200 OK sent to the UAC.

Workaround: There is no workaround.

- CSCty54718

Symptoms: A Cisco 3945 router crashes with configuration greater than 40k DN numbers of SAF/EIGRP.

Conditions: This symptom is seen with the reset of CUCM several times. The router crashes, and a memory leak is seen.

Workaround: There is no workaround.

- CSCty58992

Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

Conditions: This symptom is observed under the following conditions:

- Cluster is in v6 mode.
- A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS), which is when the issue occurs.

Workaround: There is no workaround.

- CSCty64721

Symptoms: Improper memory allocation by CTI process crashes the CME.

Conditions: This symptom occurs when the CTI front end process is using up huge memory, causing the CME to crash eventually. When the crash occurs:

```
Processor Pool Total: 140331892 Used: 140150164 Free: 181728
I/O Pool Total: 27262976 Used: 5508816 Free: 21754160
```

Workaround: There is no workaround.

- CSCty65189

Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

Conditions: This symptom is observed when ZBFW is configured.

Workaround: There is no workaround.
- CSCty77190

Symptoms: DTLS is switched back to TLS after reconnect.

Conditions: This symptom is observed with the following conditions:

 - Test image c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
 - Test version
 - Cisco IOS Release 15.2(01)T

Workaround: Restart the AnyConnect client.
- CSCty78435

Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.
- CSCty80074

Symptoms: A Cisco 3800 router running Cisco IOS Release 15.0(1)m7, with only Multilink or Serials, shows aborts and input errors during normal traffic conditions.

Conditions: This symptom is observed with normal traffic load. In addition, when a ping sweep is done, aborts and input errors are seen more frequently.

Workaround: There is no workaround.
- CSCty83520

Symptoms: IP Phone -- CUCM --- H323 -- 3845 - PSTN

 1. A call is originated from the IP phone to a PSTN number and it gets connected.
 2. The IP phone puts the call on hold.
 3. The CUCM instructs GW to listen to the Multicast MoH stream.
 4. The Cisco IOS Gateway sends the RTCP packet to Multicast MoH.

Conditions: This symptom is observed when the H.323 Gateway is configured and the Multicast MoH and MoH stream is sent across an IP Multicast network.

Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS.

Workaround 2: Use Unicast MoH.
- CSCty84512

Symptoms: All Wi-Fi phones are stuck in “Connecting...”.

Conditions: This symptom is observed with Wi-Fi phones connected to Cisco UC540W/UC520W AP.

Workaround: Power cycle the phone.

- CSCty86111

Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

Conditions: This symptom is observed with Cisco ISR G2 router.

Workaround: There is no workaround.

- CSCty90293

Symptoms: Processing improvements for GREv6 over IPv6 currently require IP CEFv6 to be disabled.

Conditions: This symptom is observed with GREv6 over IPv6.

Workaround: Use “tunnel protection” instead.

- CSCty96052

Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

Conditions: This symptom is an extreme corner case/timing issue. This issue has been observed only once on a release image.

Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty97255

Symptoms: High CPU is seen under “rf task” after a reload or an upgrade.

Conditions: This symptom is observed on Cisco ISR routers configured with “crypto map redundancy”.

Workaround: Remove “crypto map redundancy”.

- CSCtz13818

Symptoms: In a rare situation when route-map (export-map) is updated, Cisco IOS is not sending refreshed updates to the peer.

Conditions: This symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then, Cisco IOS does not send refreshed updates with modified route-targets.

Workaround 1: Refresh the updated route-target to use **clear ip route vrf vrf-name net mask**.

Workaround 2: Hard clear the BGP session with the peer.

- CSCtz27137

Symptoms: An upgrade to the S639 or later signature package may cause a Cisco IOS router to crash.

Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:

- Cisco IOS Release 12.4(24)T4
- Cisco IOS Release 15.0(1)M4
- Cisco IOS Release 15.0(1)M8
- Cisco IOS Release 15.2(3)T

Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:

- Access the router via the console.
- Enter break sequence to access ROMmon mode.
- Change the config-register value to 0x2412.
- Boot the router to bypass the startup-configuration.
- Configure the basic IP parameters.
- TFTP a modified configuration to the router's running-configuration with Cisco IOS IPS disabled.
- Reset the config-register to 0x2102.
- Enter the **write memory** command and reload.

- CSCtz41130

Symptoms: The build failed for the Cisco 7200 platform after committing changes for CSCtj14921 to the v151_4_m_throttle.

Conditions: This symptom occurs when monolith changes are not committed.

Workaround: Commit the monolith changes to the v151_4_m_throttle.

- CSCtz42421

Symptoms: The device experiences an unexpected crash.

Conditions: This symptom is observed when Zone-Based Firewalls are enabled. H225 and H323 inspection is being done during the crash. The actual conditions revolving around the crash is still being investigated.

Workaround: There is no workaround.

- CSCtz44989

Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

Conditions: This symptom is observed with IPv6 link-local next-hop. When the EIGRP route is redistributed to BGP VRF, it clears the next-hop information (it become 0.0.0.0). Now, this route becomes invalid and BGP is not able to export to another VRF.

Workaround: There is no workaround.

- CSCtz48615

Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

Conditions: This symptom is observed with AES encryption configuration in ISAKMP policy. The issue is seen only when one of the negotiating routers is a non-Cisco device where the key size attribute is not sent in ISAKMP proposal.

Workaround: Remove ISAKMP policy with AES encryption.

- CSCtz52843

Symptoms: The following messages are displayed whenever the ATM link goes down.(Cu is deploying ADSL.)

```
Nov 2 05:27:49 EDT: %SYS-2-BADSHARE: Bad refcount in pak_enqueue,
ptr=6431A7E8, count=0,
-Traceback= 0x60BA4218 0x6035E098 0x6035FEC4 0x6064CD48 0x603676F0 0x608BABC8
0x6065D344 0x60666798
0x602D6240 0x600BA8CC 0x621D75E4 0x6004A188
```

```
Nov 2 05:27:49 EDT: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=6431A7E8, count=0,
-Traceback= 0x60BA4218 0x6035937C 0x603600C4 0x6064CD48 0x603676F0 0x608BABC8
0x6065D344 0x60666798
0x602D6240 0x600BA8CC 0x621D75E4 0x6004A188
```

```
Nov 4 08:29:27 EST: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up
```

```
Nov 4 08:29:27 EST: %SYS-4-CHUNKMALLOCFAIL: Could not allocate chunks for
ATM0/1/0
```

```
Total free: 0, Total inuse: 16, Cause : Not a dynamic chunk
-Process= "ATM Periodic", ipl= 4, pid= 65, -Traceback= 0x60BA4218 0x6027CB94
0x6027CBF8 0x603837A0
0x6027F688
```

Conditions: This symptom occurs when OAM is used to manage the PVC and the peer interface is down.

Workaround: There is no workaround.

- CSCtz59145

Symptoms: A crash occurs randomly. The following error messages are often seen before the crash:

```
Mar 31 16:30:16.955 GMT: %SYS-2-MALLOCFAIL: Memory allocation of 20 bytes
failed from 0x644DA7E0, alignment 0
Pool: Processor Free: 274176384 Cause: Interrupt level allocation
Alternate Pool: None Free: 0 Cause: Interrupt level allocation
-Process= "<interrupt level>", ipl= 1
```

```
Mar 31 16:30:16.963 GMT: %SYS-3-BADLIST_DESTROY: Removed a non-empty
list(707C0248, name: FW DP SIP dialog list), having 0 elements
```

This device is not actually running out of memory. There is a memory action going on at the interrupt level which is not allowed.

Conditions: This symptom occurs when Zone-Based Firewalls inspect SIP traffic. This issue is likely related to the tracebacks and error messages given above. The actual condition is still being investigated.

Workaround: If plausible, disabling SIP inspection could possibly prevent further crashes.

- CSCtz70938

Symptoms: When the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.

Conditions: This symptom occurs when the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.

Workaround: Do not use boot configuration files other than startup-configuration when there are “service-module” CLI in the configuration.

- CSCtz72044

Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

Conditions: This symptom is timing-dependent; therefore, the problem is not systematic.

Workaround: There is no workaround.

- CSCtz80643

Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive vrf name** command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive vrf name** command via the Virtual-Template or RADIUS profile.

Workaround: There is no workaround.

- CSCua06598

Symptoms: The router may crash with breakpoint exception.

Conditions: This symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

Workaround: Disable SNMP IPv6 polling.

- CSCua08876

Symptoms: IPv6 LCP fails to negotiate on PPP over VDSL connections on Cisco 867VAE routers. (If you have "ppp negotiation{ debug enabled, you will see a "LCP: O PROTREJ" message displayed.)

Conditions: This symptom was first seen in Cisco IOS Release 15.1(4)M4, but it has also been found to be in Cisco IOS Release 15.2(3)T.

Workaround: There is no workaround.

- CSCua43930

Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

Conditions: This symptom is observed on a Cisco ISR G2.

Workaround: There is no workaround.

- CSCua77729

Symptoms: Embedded AP in the Cisco 1941 ISR becomes unreachable after using the "reload in" command on the Cisco ISR CLI. This issue is seen when using "reload in" on the Cisco ISR CLI and choosing the option to reload embedded AP.

```
CISCO1941W-E/K9 Version 15.1(4)M4
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1
```

```
Router#reload in 10
```

```
Do you want to reload the internal AP ? [yes/no]: yes
```

```
Do you want to save the configuration of the AP? [yes/no]: no
```

```
System configuration has been modified. Save? [yes/no]: no
Reload scheduled for 13:57:01 UTC Mon May 21 2012 (in 10 minutes) by console
Reload reason: Reload Command
Proceed with reload? [confirm]
Router#
May 21 13:47:03.759:
%SYS-5-SCHEDULED_RELOAD:<http://www.cisco.com/cgi-bin/Support/Errordecoder
/index.cgi?action=search&counter=0&paging=5&links=reference&index=all&
query=SYS-5-SCHEDULED_RELOAD>
Reload requested for 13:56:51 UTC Mon May 21 2012 at 13:46:51 UTC Mon May 21
2012 by console. Reload Reason: Reload Command.
```

After that, AP becomes unreachable, and the user cannot session to AP with “service-module wlan-ap 0 session”.

Conditions: This symptom is observed when using “reload in” on the Cisco ISR CLI and choosing the option to reload embedded AP. This issue is seen under the following conditions:

```
CISCO1941W-E/K9 Version 15.1(4)M4
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1
using the "reload in" command on ISR CLI with Do you want to reload the internal AP ?
[yes/no]: yes
```

Workaround 1: Use “reload in” on the Cisco ISR CLI and do not choose the option to reload embedded AP.

```
Router#reload in 2
Do you want to reload the internal AP ? [yes/no]: no
```

Workaround 2: Use the normal **reload** command.

- CSCua99687

Symptoms: BFD does not come up with Zone-Based Firewall (ZBFW) applied on the same interface.

Conditions: This symptom is observed when BFD and ZBFW are configured on a Gigabit interface on a Cisco CGR 2010 running Cisco IOS Release 15.1(4)M4. It works fine on Cisco IOS Release 15.1(4)M.

Workaround: There is no workaround.

- CSCtw58664

Symptoms: SSL VPN for SCCP causes a crash when clearing a WebVPN session.

Conditions: This symptom is observed when using the SSL VPN for SCCP phones feature and when clearing the WebVPN session:

```
clear webvpn session context SSLVPNphone

[WV-TUNL-EVT]:[0] Returning address 10.0.112.200 to pool

Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0x2601227C

-Traceback= 0x26008B3Cz 0x25F9D7E8z 0x25F94A3Cz 0x224B66A8z 0x224BCBA8z
0x224CBF70z 0x23D22684z 0x23D189C0z 0x237F0144z 0x237F0128z -Traceback=
0x26008B3Cz 0x25FCEAA8z 0x238561D8z
```

The frequency of the issue is rare.

Workaround: There is no workaround.

- CSCtu29881

Symptoms: A router may crash while using double authentication for IPsec (ESP + AH) and certain types of traffic. The following message is seen in the crashinfo file:

```
validblock_diagnose, code = 1

current memory block, bp = 0xZZZZZZZZ,
memorypool type is I/O
data check, ptr = 0xZZZZZZZZ

next memory block, bp = 0xZZZZZZZZ,
memorypool type is I/O
```

```
data check, ptr = 0xZZZZZZZ

previous memory block, bp = 0xZZZZZZZ,
memorypool type is I/O
data check, ptr = 0xZZZZZZZ
```

The router crashes due to I/O memory corruption - block overrun.

Conditions: This symptom is observed with double authentication (AH + ESP) and certain type of packets.

Workaround 1: Do not use double authentication (AH + ESP). Use ESP instead.

Workaround 2: Use an IOS version that does not have the fix for CSCtc40806.

- CSCtk74632

Symptoms: In some rare scenarios, closed IPC connections may be still detected as active, and cause some IPC message pass to fail.

Conditions: This symptom is observed in rare scenarios in which IPC connections are being set up and torn down frequently.

Workaround: There is no workaround.

- CSCtu07968

Symptoms: A Cisco 890 router may provide incorrect performance monitor statistics and omit some incoming packets from being handled by flexible netflow.

Conditions: This is observed when performance monitoring or flexible netflow is enabled with IPsec over a tunnel on an input interface.

Workaround: There is no workaround.

- CSCty54695

Symptoms: RRI routes are missing when IPsec SA is up after peer IP change.

Conditions: This symptom is observed under the following conditions:

- Cisco ASR 1002 router running Cisco IOS XE Release 3.4.2S.
- Dynamic crypto map with RRI.
- Peer changes the IP address frequently.

Workaround: Clear the crypto session with the peer.

- CSCty97961

Symptoms: A device configured with SSLVPN crashes.

Conditions: This symptom is observed when a device configured is with SSLVPN and **functions svc-enabled** or **functions svc-required** and **svc dtls**, and has an outbound ACL on one of the device's interface.

This vulnerability has only been observed when the outbound ACL is tied to either a NAT or ZBFW interface in the outbound direction and is not the interface that the SSLVPN session is terminated against.

This vulnerability has only been observed when the SSLVPN sessions terminate over PPP over ATM interface.

This vulnerability was not able to be reproduced over SSLVPN sessions terminating over Ethernet or Serial interfaces.

Workaround: Remove the outbound ACL, or **no svc dtls** if running Cisco IOS software that has a fix for CSCte41827.

- CSCty99846

Symptoms: Cisco IOS software includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

CVE-2009-1386

This bug was opened to address the potential impact on this product.

Conditions: This symptom is observed when a device is configured with SSLVPN and **svc dtls**.

Workaround: Disable DTSL with **no svc dtls**.

Further Problem Description: This problem would only be seen in Cisco IOS when using Anyconnect client with Cisco IOS SSLVPNs, after the initial session has been authenticated and established. Exploitation would result in Cisco IOS reloading.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C>

CVE ID CVE-2009-1386 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCua31157

Symptoms: One-way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. This issue is only seen intermittently.

Logs on the spoke that fail to receive the traffic show "Invalid SPI" error messages exactly one minute after the tunnel between the spokes came up.

Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T1.

Workaround: There is no workaround.

- CSCua93688

Symptoms: When pinging from the Cisco 1921 router to connected devices, the response time is unexpectedly slow.

round-trip min/avg/max = 8/46/92 ms

Conditions: This symptom is observed with the EHWIC-1GE-SFP-CU module on Cisco ISR-G2 platforms.

Workaround: Shut/no shut the EHWIC-1GE-SFP-CU interface. The ping time resumes to normal.

- CSCub39997

Symptoms: SIP TNP phones failed to register with CME.

Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M4.14.

Workaround: There is no known workaround.

- CSCtz58719

Symptoms: Watchdog timeout is seen under interrupt or process.

Conditions: This symptom is observed with a QoS configuration applied. The issue happens because of resource contention between a process path packet and an interrupt path packet.

Workaround: Disable QoS.

- CSCtl05570

Symptoms: SNMP does not work on the ppc/mips/x86 PI image.

Conditions: This symptom does not occur every time. When this issue is seen, SNMP will stop working even after reload/power cycle of the router.

Workaround: The only way to make SNMP work again is manually start [nova-k5-7:~]\$ /usr/binos/bin/snmp_subagent.

Resolved Caveats—Cisco IOS Release 15.1(4)M4

Cisco IOS Release 15.1(4)M4 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M4 but may be open in previous Cisco IOS releases.

- CSCsg48725

Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

```
TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
```

Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCtd86428

Symptoms: SSH session does not accept IPv6 addresses in a VRF interface, but will accept IPv4 addresses.

Conditions: The symptom is observed when you specify the VRF name with an SSH that belongs to an IPv6 interface.

Workaround: You can specify the source interface.

Further Problem Description: SSH sessions not accept IPv6 addresses in VRF interface, but accepts IPv4 address:

- Telnet session accepts both v6 and v4 addresses in VRF interface.
- “Destination unreachable; gateway or host down” message shows in SSH session to IPv6 address in VRF interface.

- CSCtl53576

Symptoms: A Cisco router freezes while executing the **show run** command.

Conditions: This symptom is observed if “auto ip sla schedule” is configured on the router.

Workaround: There is no workaround.

- CSCtn07696

Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

Conditions: This symptom is observed with the following CLI:

```
show tech-support | redirect
ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
```

During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn36227

Symptoms: Alignment errors or 'C' response may occur in response to IPv6 pings.

Conditions: These symptoms may be observed while sending an IPv6 ping.

Workaround: There is no workaround.

- CSCtn56006

Symptoms: The SNMP value is not matching with the output value of the **show** command.

Conditions: This symptom is observed under no specific condition.

Workaround: There is no workaround.

- CSCtn65116

Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Cisco IOS Release 12.2(33)SRB or later. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, e.g.: 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). It is seen with the following process:

1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
2. The allocated label changes from 16 to 17, e.g.: due to interface flapping or BGP attribute change.
3. However, before the BGP import happens, a more specific prefix (e.g.: 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, RT policy.

Workaround: Remove RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCto59459

Symptoms: Connections that are optimized by WAAS are reset. Malformed TCP options are added to the packet that is created and sent by WAAS-Express over the WAN, causing the peer WAE to reset connections.

Conditions: Any TCP connection will suffer from this defect.

Workaround: There is no workaround.

- CSCto90912

Symptoms: A crash is seen with the DHCPv6 client process.

Conditions: The symptom is observed when **ipv6 address dhcp** is run on an "auto-template" interface, and then the interface is removed with a **no int auto-temp**.

Workaround: There is no workaround.

- CSCto93880

Symptoms: Enable authentication fails when user is configured with TACACS server group.

Conditions: This symptom occurs when TACACS server is configured with user defined group and configured for enable authentication. User is unable to authenticate when he tries to switch to privilege executive mode (enable) and gets the following error that indicates that there is no address for defined servers.

```
%TAC+: no address for get_server
%TAC+: no address for get_server
```

Workaround: Configure the TACACS server group with the default group name.

- CSCtq59923

Symptoms: OSPF routes in RIB point to an interface that is down/down.

Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

Workaround: Configure the **ip routing protocol purge interface** command.

- CSCtq74389

Symptoms: While using a Switch Virtual Interface (SVI) as a Layer 2 Tunnel Protocol Version 3 (L2TPv3) termination, the SVI interface floods an unknown unicast packet unexpectedly.

Conditions: This symptom is observed while using an SVI interface as an L2TPv3 termination.

Workaround: Use a routed port instead of an SVI.

- CSCtq77024

Symptoms: Metrics collection fails on hop0 if route change event occurs.

Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.

Workaround 1: Remove and reschedule mediatrace session.

Workaround 2: Remove and reconfigure mediatrace responder.

- CSCtq92650

Symptoms: DMVPN tunnel is not selecting the right source interface.

Conditions: The symptom is observed when multi-link frame relay creates more than one sub-interface with the same name.

Workaround: There is no workaround.

Further Problem Description: This bug resolves the issue reported in CSCth08338 for Cisco IOS Release 15.1M.

- CSCtr18985

Symptoms: The CEF adjacency for a Frame Relay point-to-point circuit is incomplete causing the traffic passing through the Cisco router to drop.

Conditions: This symptom is observed after the Cisco router reloads.

Workaround 1: Flap the Serial interface.

Workaround 2: Disable CEF either on the serial interface or globally.

- CSCtr25734

Symptoms: A router crashes.

Conditions: This symptom is observed when the router is reloaded with a BRI interface brought up in startup configuration.

Workaround: There is no workaround.

- CSCtr86077

Symptoms: MGCP call drops 10 seconds after IP phone puts call on hold.

Conditions: The symptom is observed under the following conditions:

- IP phone -- CUCM -- MGCP -- GW -- PRI.
- **mgcp rtp unreachable timeout 10000** is configured on gateway.
- **no MOH** is configured for the IP phone so Tone on Hold (TOH) is used.
- IP phone make calls to PSTN and is answered.
- IP phone puts call on hold.
- PSTN user hears TOH.
- 10 seconds after hold is initiated, the call is dropped.

Workaround: Remove **mgcp rtp unreachable timeout** from the MGCP gateway.

- CSCtr86149

Symptoms: A router crashes if placing a call from an ISDN phone to an IP phone. The call is a secure SIP call (TLS); the phone is also using secure SCCP.

Conditions: The router is in secure SRST mode due to a WAN outage.

Workaround: There is no workaround.

- CSCtr88739

Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove **import-route target** and reconfigure route-target.

Workaround for symptom 2: Clear **ip route x.x.x.x** to resolve the issue.

- CSCts46578

Symptoms: Firewall may drop a packet with log similar to:

```
%FW-6-DROP_PKT: Dropping ftp-data session 10.7.7.99:1449 10.7.8.100:20 due
to Invalid Seq# with ip ident 6621 tcpflags 0x8018 seq.no 3558493868 ack
1386495675
```

Retransmitted packet is allowed through.

Conditions: CBAC configured.

Workaround: There is no workaround.

- CSCts67465

Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

Conditions: The symptom is observed always, if the standby is configured as an SSO.

Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

Symptoms: A Cisco 7600 router ceases to advertise a default route configured via **neighbor default-originate** to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

Workaround: Remove and re-add the **neighbor default-originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCtt05910

Symptoms: Router crashes.

Conditions: The symptom is observed when running the **show sum** command. It is seen with the Cisco 3900e platform.

Workaround: Do not use the **show sum** command.

- CSCtt16051

Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall>

- CSCtt17879

Symptoms: The **bgp network backdoor** command does not have any effect.

Conditions: This symptom occurs:

- On 64-bit platform systems.
- When the network is learned after the backdoor has been configured.

Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt21228

Symptoms: Router crashes while trying to configure Tcl script via SSH connection.

Conditions: SSH to the router and then try to configure Tcl script.

Workaround: There is no workaround.

- CSCtt26721

Symptoms: A Cisco router may see increased CPU utilization when NBAR is used.

Conditions: This has been experienced on a Cisco 3925 router running Cisco IOS Release 15.1(3)T2.

Workaround: There is no workaround.

- CSCtt43552

Symptoms: A Cisco router reloads with the **warm-reboot** command.

Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.

Workaround: There is no workaround. Remove warm-reboot from configuration (router will not be able to use the warm reboot feature).

- CSCtu00488

Symptoms: The traffic stops in the transmit direction of GE0 (configured as WAN) interface for traffic coming from FE8 (configured as LAN) interface.

Conditions: This symptom is observed when **batch** commands are configured on GE0 and FA8 interfaces.

Workaround: Do not use **batch** commands as they are intended for performance improvement in the case of higher cache misses.

- CSCtu02542

Symptoms: T.38 OnRamp consistently fails for every call with the following error:

```
%LAPP_ON_MSGS-6-LAPP_ON_CAUSE_NO_MEMORY: No memory available
```

The debugs indicate negative free process memory while displaying the following message:

```
%LAPP_ON_MSGS-6-LAPP_ON_CAUSE_NO_MEMORY: No memory available
```

```
//1093/4DE38C71808E/FOIP_ON/lapp_on_call_handoff:
```

```
SOFTWARE_ERROR; Not enough memory; Free Process Memory Bytes=-1922868956
```

However, while monitoring memory, no issues appear with the available memory resources:

```
Router#show memory stat
```

	Head	Total (b)	Used (b)	Free (b)	Lowest (b)	Largest (b)
Processor	2AC0BEE0	2436776224	59890020	2376886204	2113970464	1034143696
I/O	C000000	67108864	20001528	47107336	46989820	46943484

Conditions: The conditions under which these symptoms are observed are unknown.

Workaround: Apply a logging buffer large enough to bring the free memory below 2147483648 (b). For example, **logging buffered 500000000**.

- CSCtu02833

Symptoms: ISR G2 with IVR crashes due to bus error exception.

Conditions: The symptom is observed with a Cisco ISR G2 that is running Cisco IOS Release 15.1(1)T2.

Workaround: There is no workaround.

- CSCtu57226

Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.

Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace>

- CSCtu06894

Symptoms: Cisco UBE crashes when the **show sip-ua calls** command is executed while there is an active SIP call through system.

Conditions: This symptom is present on Cisco 2821 routers. The router crashes only when Cisco UBE receives an SDP length greater than 9000 bytes as part of a SIP message. And at the same time, if the show command is executed, the crash occurs. Otherwise, the crash is not seen.

Workaround: There is no workaround.

- CSCtu08717

Symptoms: A Cisco router experiences a watchdog timeout while executing `tw_timer_replenish`.

Conditions: This symptom is observed on the Cisco router if the IP SLA and Performance Agent features are configured on it. This timeout may also be observed if traffic is sent for a long time through a router configured with these features.

Workaround: There is no workaround.

- CSCtu11140

Symptoms: When there is no reachability cache on a DLSw router, the DLSw router sends CUR_EX unexpectedly if receiving XID_F.

Conditions: The symptom is observed if a DLSw router receives XID_F when there is no reachability cache.

Workaround: There is no workaround.

- CSCtu11677

Symptoms: A Cisco router may unexpectedly reload due to bus error or segV exception or generate a spurious error when the `cSipStatsSuccessOkTable snmp` object is polled.

Conditions: This is seen on a voice gateway when the `cSipStatsSuccessOkTable snmp` object is polled.

Workaround: Create an SNMP view and then block the oid for `cSipStatsSuccessOkTable` and then apply it to all SNMP communities on the device:

```
snmp-server view blockmib iso include
snmp-server view blockmib 1.3.6.1.4.1.9.9.152.1.2.2.5 exclude
```

and then apply it to the community:

```
snmp-server community <community> view blockmib ro
```

- CSCtu12445

Symptoms: Traffic breaks off for a long time even though STP topology is converged on a Cisco 2921 router.

Conditions: There are two Ethernet links between two Cisco 2921 routers, one is a forwarding link, and the other one is a blocking link. This symptom is observed when the forwarding link is broken, and the blocking link takes over as the forwarding link. This causes a break in traffic.

Workaround: There is no workaround.

- CSCtu16433

Symptoms: A Cisco 3725 running Cisco IOS Release 12.4(15)T may crash in GETVPN with the following bus error. It appears to crash just after registration:

```
%GDOI-5-GM_REGS_COMPL: Registration to KS <snip> complete for
group <snip> using address <snip>
```

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC =
<snip>
```

Conditions: The symptom is observed on Cisco IOS Release 12.4(15)T14.

Workaround: There is no workaround.

- CSCtu17228

Symptoms: DHCPv6 relay does not work on an EHWIC.

Conditions: This symptom is observed when one of the following modules is used:

- EHWIC-4ESG
- EHWIC-4ESG-P
- EHWIC-D-8ESG
- EHWIC-D-8ESG-P

Workaround: There is no workaround.

- CSCtu18786

Symptoms: Device may crash showing “VOIP” error messages. Decodes point to voice functions.

Conditions: The symptom is observed when SIP is enabled on the device.

Workaround: There is no workaround.

- CSCtu21636

Symptoms: Sometime calls are dropped if there are active calls on the DSP. The following errors are displayed in the logs:

```
Power alarm on DSP channel ch=1 is ON
0001 0001 **
```

```
Power alarm on DSP channel ch=1 is OFF
0001 0000 **
```

```
Power alarm on DSP channel ch=1 is ON
0001 0001 **
```

```
Power alarm on DSP channel ch=1 is OFF
0001 0000 **
```

Conditions: This symptom is seen with all conditions.

Workaround: There is no workaround.

- CSCtu21967

Symptoms: A router configured to be an IP voice gateway may crash.

Conditions: The exact conditions for this crash are currently unknown.

Workaround: There is no workaround.

- CSCtu29107

Symptoms: While using the “Reuse MAC address” feature on an ATM RBE, the router uses the MAC address of the main interface rather than the configured MAC address of the subinterface.

Conditions: This symptom is observed when ATM route bridge encapsulation is used with the “Reuse MAC address” feature.

Workaround: There is no workaround.

- CSCtu36224

Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.

Workaround: There is no workaround.

- CSCtv21900

Symptoms: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.

Conditions: This symptom is observed under the following conditions:

- Encrypted call with SRTP
- MGCP Controlled Gateway
- Cisco IOS Release 15.1(4)M or later releases

Phone logs show the following message:

```
6622: DBG 23:29:50.256330 DSP: RTP RX: srtp_unprotect() again
6623: DBG 23:29:50.257139 DSP: RTP RX: srtp_unprotect() failed with error
code 7
6624: DBG 23:29:50.276390 DSP: RTP RX: srtp_unprotect() failed with auth func
3
```

The “Rcvr Lost Packet” counter on the Cisco IP phone begins to increment as soon as the call connects.

Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.

Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- CSCtw45055

Symptoms: A Cisco ASR series router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session Neighbor deleted
Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session Neighbor deleted
Nov 10 08:10:51.816: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
```

Exception to IOS Thread:

Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler

The scheduler process will attempt to reference a freed data structure, causing the system to crash.

Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

Workaround: There is no workaround.

- CSCtw45592

Symptoms: The **ntp server DNS-name** command is not synced to the standby device. When the **no ntp server hostname** command is issued later on the active device, the standby device reloads because the config was not added.

Conditions: This symptom is observed when the device is reloaded or when the DNS name is not resolved. Due to this, the config is not added. After the standby SYNC failure, then issue the **no ntp server hostname** command.

Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations.

- CSCtw48553

Symptoms: When MPLS-IP is configured on a Cisco router and QoS policy-map actions are applied, classification fails and packets are dropped. This prevents the committed information rate (CIR) from getting updated on the output interfaces.

Conditions: This symptom is observed on any Cisco router that is running either Cisco IOS Release 15.0(1)M7.10 or later releases, or Cisco IOS Release 15.1(4) M2.5 or later releases.

Workaround: There is no workaround.

- CSCtw56439

Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

Workaround: There is no workaround.

- CSCtw59086

Symptoms: Unable to connect via Cisco AnyConnect or the WebVPN portal on a Cisco IOS router.

The following message is seen in the Syslog:

```
%SSLVPN-6-LICENSE_NO_FREE_COUNT: All available SSLVPN session licenses are in use
```

Conditions: This symptom is observed when the WebVPN License counter incorrectly reads 4294967295. Also, no connections are visible while executing the **show webvpn session context all** command.

For example:

```
sh webvpn session context all
show webvpn license
    Max platform license count : 1500
    Available license count    : 100
    Reserved license count     : 100
* In-use count                 : 4294967295*
```

Workaround: Reload the Cisco router.

- CSCtw62213

Symptoms: When two Cisco 3945E routers are connected to each other and perform IPSLA operations, the responder experiences a drop in packets coinciding with the license update process.

Conditions: This symptom is observed when two Cisco 3945E routers are connected back to back while performing IPSLA UDP-jitter operation.

Workaround: Increase both the input queue length on the interface and the SPD queue length.

- CSCtw66863

Symptoms: A Cisco router may crash when using VXML script with Cisco proprietary tag *Cisco-data*.

Conditions: This symptom is observed when the *Cisco-data* tag uses memory beyond allocated memory, which causes the router to crash intermittently.

Workaround: There is no workaround.

- CSCtw73544

Symptoms: A leak is observed in the header pool with “ppp multilink”.

Conditions: This symptom is observed with PPP over ATM.

Workaround: There is no workaround.

- CSCtw78064

Symptoms: The **display-logout** message on a Cisco SCCP Phone is not cleared even after pressing other buttons on the phone.

Conditions: This symptom is observed on the Cisco SCCP phone (also known as Skinny Phone or ePhone) when the last extension mobility (EM) user in a hunt group logs out using the HLog button. This symptom is observed even if the last EM user logs out of the hunt group and logs back in.

Workaround: There is no workaround.

- CSCtw99290

Symptoms: The source or destination group-address gets replaced by another valid group-address.

Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

Workaround: There is no workaround.

- CSCtx06747

Symptoms: Device crashes at boot and never reaches CLI.

Conditions: This symptom will happen even with no configuration. This issue is only seen with Cisco IOS Release 15.1(4)M3 due to a bad code fix integrated. The following platforms with k9 images are impacted by this bug: Cisco AS5300, Cisco AS5400, Cisco 7200, Cisco 7200p, Cisco 7301, Cisco VGD 1T3.

Workaround: There is no workaround. Downgrade to Cisco IOS Release 15.1(4)M2, or upgrade to Cisco IOS Release 15.1(4)M3a.

- CSCtx09973

Symptoms: Voice quality on the network deteriorates after 10 minutes.

Conditions: This symptom is observed when voice traffic is not classified properly and is classified as web or other kind of traffic.

Workaround: There is no workaround. However, use ACL to correctly tag the traffic.

- CSCtx19332

Symptoms: A Cisco router crashes when 'remote mep' is unlearned while auto EOAM operations are executing.

Conditions: This symptom is observed if 'remote mep' is unlearned from the auto database (shutdown on interface or remote mep reload) while the 'IP SLA ethernet-monitor jitter' operation is still running. The crash occurs if the initial control message times out.

Workaround: There is no workaround.

- CSCtx27813

Symptoms: Evaluation license cannot be used on a Cisco router.

Conditions: This symptom is observed on a Cisco router when the evaluation license has high priority and the router is reloaded.

Workaround: There is no workaround.

- CSCtx29543

Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

Conditions: This symptom occurs under the following conditions:

1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
2. A default route exists.
3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

The router may now crash when doing **show ip route** command or when default route is updated.

Workaround: There are two possible workarounds:

1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
 2. If the previous workaround does not work, then ensure that at least one supernet route exists at all times for all possible mask lengths. For example by configuring summary routes that do not interfere with normal operation.
- CSCtx32628

Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

- BGP full mesh is configured.
- BGP cluster-id is configured.
- **address family vpnv4** is enabled.
- **address family ipv4 mdt** is enabled.
- The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx38806

Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

The problem affects Firefox also (version 10.0.1) displaying the following message:

"The page isn't redirecting properly"

Conditions: This symptom is observed in Cisco IOS software that is acting as head end for SSL VPN connections.

Workaround: Any of the following workarounds will work:

1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS software.
2. Uninstall the update.
3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

```
webvpn gateway gateway name
    ssl encryption rc4-md5
```

4. Use AC 2.5.3046 or 3.0.3054.
5. Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:

"Connection attempt has failed due to server communication errors. Please retry the connection"

The AnyConnect event log will show the following error message snippet:

```
Function: ConnectIfc::connect
Invoked Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtx49766

Symptoms: GETVPN does not allow traffic in a Cisco HWIC-3G-CDMA-V modem.

Conditions: This symptom is observed on a Cisco HWIC-3G-CDMA-V modem running Cisco IOS Release 15.1(4)M3.

Workaround: Use Cisco IOS Release 15.1(3)T3 with the Cisco HWIC-3G-CDMA-V modem.

- CSCtx51935

Symptoms: Router crashes after configuring **mpls traffic-eng tunnels**.

Conditions: The symptom is observed with the following steps:

```
interface gil/2
mpls traffic-eng tunnels
no shut

router OSPF 1
mpls traffic-eng area 100
mpls traffic-eng router-id lo0
end

show mpls traffic-eng link-management summary
```

Workaround: There is no workaround.

- CSCtx84059

Symptoms: Forwarded calls in the SIP network experience one-way audio on calls from FXS to SIP.

Conditions: This symptom is observed on a Cisco router that uses route-map for routing to the SIP network.

Workaround: Add static route to the CFU party IP address.

- CSCtx87646

Symptoms: Firmware behavior options can only be used if "service internal" is activated.

Conditions: The condition under which this symptom is observed is unknown.

Workaround: There is no workaround.

- CSCtx88093

Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.

Conditions: This symptom occurs while using the **dialer-list x protocol ip deny** command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.

Workaround: Use the method that follows to define interesting traffic instead of **dialer-list x protocol ip deny**:

```
access-list x protocol ip deny
dialer-list 1 protocol ip list x
```

- CSCty12083

Symptoms: A Cisco 819 router with the C819HG+7 SKU reloads.

Conditions: This symptom is observed on a Cisco 819 router with the C819HG+7 SKU reloads while running Cisco IOS Release 15.1(4)M3.8.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(4)M3a

Cisco IOS Release 15.1(4)M3a is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M3a but may be open in previous Cisco IOS releases.

- CSCtx06747

Symptoms: Device crashes at boot and never reaches CLI.

Conditions: This symptom will happen even with no configuration. This issue is only seen with Cisco IOS Release 15.1(4)M3 due to a bad code fix integrated. The following platforms with k9 images are impacted by this bug: Cisco AS5300, Cisco AS5400, Cisco 7200, Cisco 7200p, Cisco 7301, Cisco VGD 1T3.

Workaround: There is no workaround. Downgrade to Cisco IOS Release 15.1(4)M2, or upgrade to Cisco IOS Release 15.1(4)M3a.

Resolved Caveats—Cisco IOS Release 15.1(4)M3

Cisco IOS Release 15.1(4)M3 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M3 but may be open in previous Cisco IOS releases.

- CSCsh39289

Symptoms: A router may crash under a certain specific set of events.

Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCsk94026

Symptoms: AuthProxy sessions on a Cisco 871 router can be deleted immediately after completing the authentication.

Conditions: This issue is seen only on a Cisco 871 router. It occurs with a basic AuthProxy configuration on a BVI interface.

Workaround: There is no workaround.

- CSCso41274

Symptoms: A router crashes or shows the following traceback:

```
% Not enough DSP resources available to configure ds0-group 1 on controller T1 1/0 %
The remaining dsp resources are enough for 14 time slots. % For current codec
complexity, 1 extra dsp(s) are required to create this voice port.
sip-cme(config-controller)# %ALIGN-3-SPURIOUS: Spurious memory access made at
0x40C627A8 reading 0x4 %ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C
0x40D72E74 0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
```

Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

Example:

```
sip-cme(config)#controller t1 1/0 sip-cme(config-controller)#ds0-gr 1 time 1-16 type
e&m-imm sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-immediate-start
```

Workaround: Ensure there are more DSPs in the router than signalling channels.

- CSCta22221

Symptoms: Frame relay client triggers reload of standby router.

Conditions: This symptom occurs if many frame relay related configurations are present.

Workaround: There is no workaround.

- CSCtg06045

Symptoms: A Cisco router may reload with traceback from a crypto ACL configuration.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(15)T12 and experiencing a high CPU stress load while the ACEs are being changed periodically. This symptom is specific to the ACE entries in crypto ACL downloaded from KS.

Workaround: Simplify and consolidate the ACE entries in the crypto ACL. In addition, reducing the CPU stress level may help.

- CSCth84370

Symptoms: The Standby Supervisor gets reloaded when **write memory** is run from one VTY, and then later, **show configuration** is run from another VTY. No particular configuration needs to be done prior to **write memory**.

Conditions: This symptom occurs when the Dual Supervisor is used and the configuration file is quite long.

Workaround: Do not run the **write memory** and **show configuration** commands simultaneously.

- CSCti13493

Symptoms: A router crashes and the following traceback is seen:

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP",
ipl= 0, pid= 226, -Traceback=
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
```

Conditions: The symptom is observed with the DSMP process.

Workaround: There is no workaround.

- CSCtj21237

Symptoms: %SYS-2-LINKED: Bad enqueue, Bad dequeue messages are received, which might result in an unexpected reboot due to SegV Exception.

Conditions: The symptom is observed on a router configured with control plane policing and protection feature.

Workaround: Disable the feature in order to prevent any further crash.

- CSCtj79476

Symptoms: Traffic loss and VLAN related errors seen when the traffic is sent for a prolonged duration on an HWIC-4ESW.

Conditions: The symptom is observed when traffic is sent for a prolonged duration (>12hrs) on an HWIC-4ESW.

Workaround: There is no workaround.

- CSCtk18404

Symptoms: Per-user route is not installed after IPCP renegotiation.

Conditions: The symptom is observed with the following conditions:

1. PPP session comes up, NAS installs static routes which are sent as attribute from RADIUS server.
2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated but the static routes are lost.

Workaround: There is no workaround.

- CSCtk66753

Symptoms: On a Cisco UC560 with SSL VPN tunnel and running Cisco IOS Release 15.1(2)T2. Heavy UDP traffic through the tunnel sometimes causes the following message to be seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of 18188 bytes failed from 0x80319FD0,
alignment 32
Pool: I/O Free: 54368 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "encrypt proc", ipl= 4, pid= 249
```

The same issue is observed with Cisco IOS Release 15.1(2)T2 on a Cisco 871. With heavy UDP traffic through the SSL VPN tunnel, sometimes the following message is seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from 0x802F6A2C,
alignment 32
Pool: I/O Free: 15856 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

Conditions: The symptom is observed when you send UDP traffic (payload size=30 bytes) to SSL VPN clients through an SSL VPN tunnel.

Workaround: There is no workaround.

- CSCtl87463

Symptoms: Queue length becomes negative.

Conditions: The symptom is observed when Cisco IOS-WAAS is configured on the interface.

Workaround: There is no workaround.

- CSCtn16855
Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.
Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.
Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.
- CSCtn62287
Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.
Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.
Workaround: There is no workaround.
- CSCtn83520
Symptoms: VOIP_RTCP related traceback is seen.
Conditions: This symptom is observed when IPIP gateways are involved.
Workaround: There is no workaround.
- CSCtn87155
Symptoms: CoA sessions are not coming up.
Conditions: This symptom is observed when some CLI commands that are called within shell function might fail if the shell programmatic APIs are used.
Workaround: Manually use shell functions on the console.
- CSCto13338
Symptoms: When a PSTN phone is calling an IP Phone that is forwarded to a PSTN destination, the call is placed but no audio is present. This is the same behavior with blind transfer to external destinations.
Conditions: This symptom occurs when voice-class codec X offer all and transcoders are used with CUBE.
Workaround 1: Use the **codec XXXX** command instead of voice-class codec X offer all.
Workaround 2: Use consultative transfer instead of blind transfer.
- CSCto32044
Symptoms: The interface hangs and fails to pass traffic. It will still show an “up/up” status but the input and output rates will go to 0. The following errors will be seen:

```
%SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status = 0x0000040000000000
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to reset
```

The interface number will vary.
Conditions: The conditions are unknown.
Workaround: There is no workaround.

- CSCto89536

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfb>

- CSCto98212

Symptoms: When RIPng is removed from an interface from telnet and serial console sessions at the same time, it causes the routers to crash.

Conditions: This symptom occurs when RIPng is configured on an interface and two users are connected using two different console sessions.

Workaround: Do not configure the same RIPng through two different console sessions.

- CSCtq24614

Symptoms: The commands to ignore S1 bytes are not supported on an ATM interface.

Conditions: The symptom is observed with an ATM SPA.

Workaround: There is no workaround.

- CSCtq24733

Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.

Conditions: The symptom is observed with MRCP is enabled.

Workaround: There is no workaround.

- CSCtq45553

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfb>

- CSCtq61128

Symptoms: Router is crashing with Segmentation fault(11)

Conditions: It was observed on routers acting as IPSEC hub using certificates.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2011-4231 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtg63625

Symptoms: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4 is not getting trained with some DSLAMs without "line rate" configured manually. It gets trained with a manual line rate configured.

Conditions: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4.

Workaround: There is no workaround.

- CSCtg63838

Symptoms: A Cisco 2921 router crashes, and the following traceback is seen:

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 315556E0. -Process= "DSMP",
ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z 0x24A19810z 0x24A5DC8Cz
0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
23:50:00 UTC Sun May 1 2011: TLB (load or instruction fetch) exception, CPU signal 10,
PC = 0x2581FB94
```

Conditions: This symptom is observed with the DSMP process.

Workaround: There is no workaround.

- CSCtg64987

Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.

Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace>

- CSCtg88777

Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq90054

Symptoms: **ip nbar protocol-discovery** fails to recognize Skype application traffic.

Conditions: The issue is seen after configuring PfR to control NBAR based application traffic.

Workaround: There is no workaround.

- CSCtq91939

Symptoms: Intermittent crash due to SegV Exception after a consult transfer of external SIP call to a local ephone extension.

Conditions: The symptom is observed under the following conditions:

- UC540 that is running Cisco IOS Release 15.1(2)T3.
- CME 8.1.
- SIP---UC540---switch---SCCP---IP phones.

Workaround: There is no workaround.

- CSCtq97991

Symptoms: ADSL interface fails to re-train when “dsl enable-training-log” is configured.

Conditions:

1. Observed in a Cisco 800, 1900, and 2900 chassis and could affect other software platforms.
2. Observed in Cisco IOS Release 15.1(2)T, Release 15.1(2)T1, and Release 15.1 (3)T.
3. It is not observed in Cisco IOS Release 15.0(1)M4.

Deviation observed in the following manner:

1. With “dsl enable-training log” not configured the HWIC trains up to the DSLAM OK. After unplugging cable and reconnecting it, the HWIC still comes up fine after.
2. Configure “dsl enable-training log”. After unplugging cable and reconnecting it, the HWIC fails to come up. CD LED does not blink and the following error message appears: “No retrain. sleep 20 seconds”.

Workaround: Remove “dsl enable-training-log.”

- CSCtr04829

Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

Conditions: This symptom occurs when the hardware address is zero.

Workaround: There is no workaround.

- CSCtr06747

Symptoms: ISIS neighborship remains in INIT state when MTU at both ends is changed to 4470.

Conditions: The symptom is observed when a Cisco 2900 is used in the topology with MTU 4470 (any MTU >2000).

Workaround: Replace the Cisco 2900 with a Cisco 2800 or reduce the MTU to <2000.

- CSCtr07142

Symptoms: A memory leak is seen at crypto_ss_open.

Conditions: No special configuration is needed.

Workaround: There is no workaround.

Further Problem Description: At bootup, when the **show memory debug leaks** command is run, memory leak entries are seen for the crypto_ss_open process.

- CSCtr18574

Symptoms: H323-H323 video calls fail with cause code 47.

Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:

```
Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
cch323_send_passthru_out: Send passthru message retcode 15
```

Workaround: There is no workaround.

- CSCtr20762

Symptoms: L3VPN tunnel is not coming up after the router is reloaded.

Conditions: The symptom is observed with “aaa system accounting” configured and when the TACACS server is not reachable.

Workaround 1: Disable “aaa system accounting”.

Workaround 2: Ensure the TACACS server is reachable.

- CSCtr33856

Symptoms: Traceback and/or watchdog crash, with decodes pointing to mace_monitor_waas_command@

```
%SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 218959117 for chunk 6527D73C, data
D0D0D0D -Process= "Exec", ipl= 0, pid= 373 -Traceback= 23054C68z 2238121Cz 223877F0z
22397A24z 2376B0FCz 2376B0E0z or %SYS-2-FREEBAD: Attempted to free memory at 4F, not
part of buffer pool -Traceback= 24F4EA90z 23789608z 237758E4z 23054C68z 2238121Cz
223877F0z 22397A24z 2376B0FCz 2376B0E0z %SYS-2-NOTQ: unqueue didn't find 4F in queue
28275D8C -Process= "Exec", ipl= 4, pid= 374
```

Conditions: The symptom is observed with on the fly changes to mace policies and classes.

Workaround: There is no workaround.

- CSCtr45978

Symptoms: Cisco IOS WAAS has FTP connections hung in CONN_ABORT state.

Conditions: Device configured with Cisco IOS WAAS, and crafted FTP packets are passed across the WAN link. Has only been observed on 15.2(1)T IOS Code. Once the connection limit is reached and the rest of the connections started going pass-through.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:P/A:N/E:F/RL:OF/RC:C>

No CVE ID has been assigned to this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr46123

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

- CSCtr50118

Symptoms: The router crashes.

Conditions: This symptom occurs when the presence feature is turned on.

Workaround: There is no workaround.

- CSCtr51926

Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

Conditions: The symptom is observed when a service-policy is applied on the main interface.

Workaround 1: Enable IPv6 explicitly on the main interface:

interface x/y ipv6 enable

Workaround 2: Reconfigure the IPv6 address on the subinterface:

interface x/y.z no ipv6 address ipv6 address ...

- CSCtr52740

Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.

Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- CSCtr54327

Symptoms: A Cisco router may crash due to a SegV exception or have a spurious access when a fax comes in.

Conditions: The crash occurs on a voice gateway that is configured with transcoding and fax passthrough where a fax call comes in for a codec, but the fax is not configured for a codec, and the “a=silenceSupp:off” option is set in SDP.

Workaround: There is no workaround.

- CSCtr58658

Symptoms: VSA crypto engine reports “Deny Jump overflow” when packet match deny entries that are supposed to be sent clear.

Conditions: This problem only occurs with a Cisco 7200 with a VSA crypto engine module, where there are many crypto maps. Many of them use deny ACL, and many permit/deny crypto ACL entries share either the same source or the same destination address.

Workaround: Do not use deny entries. The traffic that does not match permit entries will automatically send clear.

- CSCtr59840

Symptoms: Crypto tunnels may flap up and down constantly after issuing a **clear crypto session** or **clear crypto isakmp** and **clear crypto sa**.

```
RTR#clear cry sess RTR# %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer
10.10.1.1:500 Id: serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN,
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer 10.10.10.10:500 Id:
serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN, RTR#
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP . Peer 10.10.1.1:500 Id:
serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN, %CRYPTO-5-SESSION_STATUS:
Crypto tunnel is UP . Peer 10.10.10.10:500 Id:
serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN, ...
```

Conditions: This issue is seen when using eToken and OCSP revocation check on Cisco 870, 881, 1812 and 1921 routers that are running Cisco IOS Release 15.1 (2)T3. Certificate-based authentication is also used.

Workaround: Disabling OCSP revocation check, if configured, may alleviate this behavior.

- CSCtr66487

Symptoms: Packet drops beyond 1492 MTU size with MPLS L2VPN Xconnect configuration.

Conditions: The symptom is observed when you ping mpls pseudowire 10.0.0.1 101 size 1493 and above.

Workaround: There is no workaround.

- CSCtr67852

Symptoms: Invalid route entries injected by the RRI mechanism after an HSRP failover happens in a stateful IPsec HA setup.

Conditions: The symptom is observed following a failover in a stateful IPsec HA setup and the use of RRI.

Workaround: Clear all crypto sessions with **clear crypto session** or remove and add back the crypto map to the interface where it is applied.

- CSCtr72393

Symptoms: Virtual-access goes down whenever you apply a service-policy to the dialer interface.

Conditions: The symptom is observed when you apply a service-policy to the dialer interface.

Workaround: There is no workaround.

- CSCtr72685

Symptoms: Keyserver is sending rekey for all groups after a change.

Conditions: Keyserver is configured for multiple GDOI groups. A change is made (e.g. ACL, sa receive only) triggering a rekey. The rekey is being sent to all the groups instead of the impacted one(s). This was observed on Cisco IOS Release 12.4(24)T, 15.0M, and 15.1M.

Workaround: There is no workaround.

- CSCtr79347

Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
Traceback summary
% 0x80e7b6 : __be_bgp_tx_walker_process
% 0x80e3bc : __be_bgp_tx_generate_updates_task
% 0x7f8891 : __be_bgp_task_scheduler
```

Conditions: No conditions but this is a rarely observed issue.

Workaround: There is no workaround.

- CSCtr83533

Symptoms: When you check the message on a VM system and that triggers the SIP notify to turn off the MWI to IAD, IAD will turn off the MWI but, after that, DSP is not released for the port. If you make one more call, in the next call you will hear silence. After it is off hook, there is no ring tone.

Conditions: The symptom is observed when MWI is configured for analog ports on IAD, and if MWI is ON and a call is made to clear the MWI.

Workaround 1: Reload the router.

Workaround 2: Remove the MWI configuration from the analog port configuration.

- CSCtr86437

Symptoms: NAT-PT function does not work properly after an interface flap occurs.

Conditions: The symptom is observed when you configure NAT-PT on the router.

Workaround: Reconfigure “ipv6 nat prefix.”

- CSCtr86666

Symptoms: EIGRP flap due to retry limit exceeded. On peer it is waiting for INIT ACK and complains of out of order sequence number.

Conditions: DMVPN network with a spoke running Cisco IOS Release 15.1(4)M.

Workaround: There is no workaround.

- CSCtr87413

Symptoms: Static route that is injected by “reverse-route static” in crypto map disappears when the router receives the delete notify from the remote peer. Static route also gets deleted when DPD failure occurs.

Conditions: The symptom is observed when you configure “reverse-route static” and then receive a delete notify or DPD failure.

Workaround: Use **clear crypto sa**.

- CSCtr92779

Symptoms: Call scenario is with Avaya CM6 over TLS/SIP trunks which causes the Cisco 3945 router (running Cisco IOS Release 15.1(4)M1) CUBE to crash.

Conditions: The symptom is observed when a call is originated from Cisco Phone A via TLS/SIP Trunk to CUBE (3945 15.1(4)M1), to Avaya CM6 Phone A which is set to “call forward all” back to the original Cisco Phone A.

Workaround: There is no workaround.

- CSCtr94471

Symptoms: Carrier specific exec commands under cellular interface, such as profile configuration and activation commands, return an error.

Conditions: The symptom is observed after the router boots up.

Workaround: There is no workaround.

- CSCtr97248

Symptoms: Router reloads with the following:

```
Unexpected exception to CPU: vector 300, PC = 0xZZZZZZZZ , LR = 0xFFFFFFFF -Traceback=
0xZZZZZZZZ
```

Conditions: The symptom is observed with L4F (TCP Proxy) based NAT ALG processing of TCP DNS traffic.

Workaround: Use the following configuration:

```
Router(config)# no ip nat service tcp-alg
```

- CSCts00341

Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server server.domain.com**, the command fails with the following message on the console:

```
ASR1k(config)#ntp server server.domain.com <<< DNS is not resolved with dual RPs on
ASR1k Translating "server.domain.com "...domain server (10.1.1.1) [OK]
%ERROR: Standby doesn't support this command ^ % Invalid input detected at '^' marker.
ASR1k(config)#do sh run | i ntp ASR1k(config)#
```

Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts11594

Symptoms: A mediatrace session is scheduled with an attached session-parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.

On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.

Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.

Workaround: Use either the default session-parameters or custom session-parameters. Do not toggle between both.

- CSCts11743

Symptoms: A Cisco router acting as a Call Manager Express device may unexpectedly reboot due to stack corruption.

Conditions: The symptom is observed if more than eight calls are being queued in a route point, and one agent transfers a call back to this route point's queue.

Workaround: From UCCX, set the limit of calls in the queue to eight.

- CSCts12366

Symptoms: Memory may not properly be freed when malformed SIP packets are received on the NAT interface.

Conditions: None.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C>

CVE ID CVE-2011-2578 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts16285

Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts18257

Symptoms: MGCP modem passthru call is failing.

Conditions: The issue is observed on a Cisco AS5400 that is running Cisco IOS Release 15.1(4)M.

Workaround: Use Cisco IOS Release 15.0(1)M6, if possible.

- CSCts24348

Symptoms: PBR "set vrf" feature can cause unnecessary ARP requests and packet drops if some other feature is configured on the same router interface and packets are punted to process-switching path. This issue slows down TCP traffic considerably as first SYN in a flow may always be dropped.

Conditions: The symptom is observed with multi-VRF selection using the Policy Based Routing (PBR) feature. It was observed in all IOS versions with new CEF code (Cisco IOS Release 12.4(20)T and upwards). The issue was not seen in Cisco IOS Release 12.4(15)T and Release 12.4(25).

Workaround: This issue can be alleviated by using proxy ARP on the upstream device. Otherwise, there is no workaround.

- CSCts27042

Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

Workaround: There is no workaround.

- CSCts28315

Symptoms: A DHCP PD request does not accept a specific server.

Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

<http://tools.ietf.org/html/rfc3633#section-10>

A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

Workaround: There is no workaround.

- CSCts30143

Symptoms: CPE WAN Management Protocol (CWMP) function is not working on UC500 platforms.

Conditions: The symptom is observed under normal operation.

Workaround: There is no workaround.

- CSCts31111

Symptoms: Coredump generation fails on the Cisco 800.

Conditions: This symptom occurs when coredump is configured.

Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

```
conf t
config-reg 0x0
end
wr
reload
yes
<rommon prompt>
DISABLE_WATCHDOG=yes
sync
set
conf-reg 0x2102
reset
```

- CSCts38291

Symptoms: When configuring 6VPE, you may see prefix corruption. Advertised prefix is different than the one installed. RD value also changes as well.

Conditions: The symptom is observed when configuring “vpnv6 address family”.

Workaround: There is no workaround.

- CSCts38429

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike>

- CSCts38674

Symptoms: UUT/modem fails to make a call using external dialer interface.

Conditions: The symptom is observed when the cellular interface is configured with “no ip address” and when using an external dialer interface, UUT/modem will fail to make a call.

Workaround: Configure cellular interface with “ip address negotiated”.

- CSCts40771

Symptoms: Device goes into a hang state and requires a power cycle. If “scheduler isr-watchdog” is configured, the device will crash and reload the system.

Conditions: This issue has been seen with “ip nbar protocol-discovery” configured on tunnel interfaces.

Workaround: Remove “ip nbar protocol-discovery” from the device.

- CSCts64539

Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts76410

Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts78348

Symptoms: Packet drop will occur on a router when the interface is configured as 10/full.

Conditions: It seems that when interface is configured as 10/full, with the traffic of 10 Mbps, this issue will occur. By performing a shut/no shut on the interface, this issue will recover but it will be seen again when you reload the device.

This issue may be seen on a Cisco 19xx and a Cisco 29xx (except Cisco 2951) This issue may occur when manual set duplex on the affected platform.

Workaround 1: Perform a shut/no shut on the interface and this issue will recover.

Workaround 2: Use auto negotiation.

- CSCts80643

Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

A workaround is available to mitigate this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp>

- CSCts99818

Symptoms: Traceback is seen.

Conditions: The symptom is observed when multimode ADSL/VDSL CPE configuration is rapidly changed between VDSL and ADSL mode while using a VDSL2-only transmission mode profile on DSLAM.

Workaround: There is no workaround.

- CSCtt07878

Symptoms: A Cisco 7206 router running IPSec sees this message in syslog output:

WARNING: start sending an incomplete HAPI bundle with errors

Conditions: The symptom is observed with a Cisco 7206 router that is running IPSec with Cisco IOS Release 15.0(1)M4.7 or higher.

Workaround: There is no workaround.

- CSCtt11210

Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt20215

Symptoms: Controller goes down after reload.

Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

Workaround: Unplug/plug the cable, or reset link from PBX side.

- CSCtt26074

Symptoms: Memory leak with IP SLAs XOS Even process.

Conditions: The symptom is observed with IP SLA configured.

Workaround: There is no workaround.

- CSCtt28703

Symptoms: VPN client with RSA-SIG can access a profile where the CA trustpoint is not anchored

Conditions: Use of RSA-SIG.

Workaround: Restrict access by using a certificate-map matching the right issuer.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RL:W/RC:C>

No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtt36513

Symptoms: Crash seen on a Cisco ASR for the process IPSec key engine.

Conditions: The symptom is observed when you have more than 4K sessions up on the ASR.

Workaround: There is no workaround.

- CSCtt47007

Symptoms: Router is unstable and displays badshare error messages in the syslog:

```
-Traceback= 60DE2A40z 60DE40C8z 602D1E30z 60F36DA4z 60F17894z *Oct 19 11:31:59.358:
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=69B9D3FC, count=
```

Conditions: Has been seen on a Cisco ISR 3845 with AIM-SSLV3. It may also show on other platforms as well.

Workaround: Disable WebVPN CEF and reload the router.

- CSCtt96597

Symptoms: Unable to power-cycle modem using **test cellular unit modem-power-cycle**.

Conditions: The symptom is observed when a router cannot communicate with the modem due to a possible modem firmware crash or device disconnect.

Workaround: Reload router.

- CSCtt97905

Symptoms: Multiple demandNbrCallDetails traps generated.

Conditions: Multiple demandNbrCallDetails traps are generated for connect under normal conditions.

Workaround: There is no workaround.

- CSCtt98801

Symptoms: Mobile router reports stale RRP received from HA.

Conditions: The symptom is observed when the mobile router sends a RRQ to HA in CCOA mode.

Workaround: There is no workaround.

- CSCtu02835

Symptoms: Slow performance through the fastethernet WAN ports while running Cisco IOS Release 15.1(4)M2.

Conditions: When the issue occurs the fastethernet WAN ports are showing a large number of throttles in the **show interface** command. The symptom only occurs when the **scheduler interval** command is configured.

Workaround: Remove the **scheduler interval** command.

- CSCtu07626

Symptoms: Router processing SIP traffic crashes.

Conditions: The following error may be seen prior to the crash:

```
%SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to process.
```

Workaround: There is no workaround.

- CSCtu13446

Symptoms: High CPU utilization will be seen on Cisco 39xxE platforms if an SM-2GE-SFP module is plugged in.

Conditions: The symptom is observed when a SM-2GE-SFP module is plugged in.

Workaround: There is no workaround.

- CSCtu36562

Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW-MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).

Conditions: The symptom is observed with failed IKE negotiations (ph1 or ph2).

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(4)M2

Cisco IOS Release 15.1(4)M2 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M2 but may be open in previous Cisco IOS releases.

- CSCso46409

Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM-VPN/SSL-3.

Workaround: There is no workaround.

- CSCta93316

Symptoms: Memory leaks are seen.

Conditions: The symptom is observed after the coop functionality test when using the **show memory debug incremental leaks** command.

Workaround: There is no workaround.

- CSCtb55479

Symptoms: A router may crash by the “BGP Router” process.

Conditions: This symptom is observed if the memory is corrupted.

Workaround: There is no workaround.

- CSCtd10735

Symptoms: A router crashes with a Cisco 7200 platform image.

Conditions: Configuring the sgbp test commands as given in the “Steps to reproduce” enclosure.

Workaround: There is no workaround.

- CSCtd15853

Symptoms: When removing VRF configuration on remote PE, local PE receives withdraw message from remote PE to purge its MDT entry. However, local PE does not delete the MDT entry.

Conditions:

- mVPN is configured on PE router.
- Both Pre-MDT SAFI and MDT-SAFI IOS are running in a Multicast Domain.

CCO : MDT SAFI

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

Workaround: There is no workaround.

- CSCtg42271

Symptoms: A router that is running Cisco IOS Release 15.0(1)M1 may experience a series of spurious memory access errors and a bus error when configured for IPS:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0XXXXXXXXX reading 0XXXX
%ALIGN-3-TRACE: -Traceback= 0XXXXXXXXX 0XXXXXXXXX 0XXXXXXXXX 0XXXXXXXXX 0XXXXXXXXX
0XXXXXXXXX
%ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
ra=0xFFFFF331z , sp=0x28F88EB0
%ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
ra=0xFFFFF331z , sp=0x28F88EB0
XX:XX:XX XXX XXX XX XXXX: TLB (store) exception, CPU signal 10, PC = 0XXXXXXXXX
```

Conditions: The symptom is observed when the device is configured for IPS and is running Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

- CSCth11006

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCth80642

Symptoms: IOS SSLVPN fails to accept new ssl connection. Sessions get stuck in Time Wait until TCP queue is full.

Conditions: SSLVPN on IOS.

Workaround: clear tcp tcb * will clear Time Wait sessions.

- CSCti33159

Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.

Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.

Workaround: There is no workaround.

- CSCtj47822

Symptoms: The standby RP is stuck in standby_issu_negotiation_late state after a switchover and does not come to SSO. Also, memory leaks are seen at tid_cmn_add_or_find_port_info.

Conditions: This symptom occurs during the peer (standby RP) reset or switchover.

Workaround: There is no workaround.

- CSCtj56551

Symptoms: The Cisco 7600 crashes in a very rare case.

Conditions: This symptom is observed very rarely when route-churn/sessions come up.

Workaround: There is no workaround.

- CSCtj95685

Symptoms: A router configured as a Voice Gateway may crash while processing calls.

Conditions: This symptom is observed with a router configured as a Voice Gateway.

Workaround: There is no workaround.

- CSCtk34885

Symptoms: Crosstalk being heard intermittently on inbound calls.

Conditions: Inbound calls from PSTN to Ingress gateway hearing crosstalk on Rout call leg (DSP to PSTN) on AS5400XM.

Workaround: The following command in IOS can mitigate this for SIP:

voice service voip sip source filter

This eliminates the risk for crosstalk since the gateway blocks all rogue audio out to the PSTN with this command.

The above command only works for SIP, so H323, MGCP, and SCCP are still affected.

The following enhancement requests have been filed:

CSCtq47019 - support on H.323, SCCP, and MGCP. This will allow the command to be used in all VoIP environments.

CSCtq47431 - To get this feature added to IP phones.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.8/1.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:H/Au:N/C:P/I:N/A:N/E:F/RL:W/RC:C>

No CVE ID has been assigned to this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtk69114

Symptoms: RP resets while doing ESP reload with crypto configuration.

Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

Workaround: There is no workaround.

- CSCtk98248

Symptoms: An FA8 line protocol goes down after the connected device is reloaded.

Conditions: The symptom is observed with the following conditions:

- A Cisco 892 router that is running Cisco IOS Release 15.0(1)M3 or earlier.
- The Cisco 892 is the only FA8 port and is set to 10/full.
- A Cisco 3750/2960 router that is running a Cisco IOS Release other than Cisco IOS Release 12.2(37)SE.

Workaround 1: Set the FA8 to 100/full or auto.

Workaround 2: Use Cisco IOS Release 15.0(1)M4 on the Cisco 892.

Workaround 3: Use Cisco IOS Release 12.2(37)SE on the Cisco 3750/2960 router.

- CSCtl00995

Symptoms: Cisco ASR 1000 series routers with 1000 or more DVTIs may reboot when a shut/no shut operation is performed on the tunnel interfaces or the tunnel source interfaces.

Conditions: This symptom occurs when all the DVTIs have a single physical interface as tunnel source.

Workaround: Use different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as tunnel source.

- CSCtl01141

Symptoms: cswmMvrfStatsTable does not get populated.

Conditions: This symptom occurs when the multicast vrf instance is configured on any switch running mtrose image and mibwalk is configured on cswmMvrfStatsTable.

Workaround: There is no workaround.

- CSCtl23748

Symptoms: EoMPLS over GRE (DMVPN) with IPSec protection is not working after a reboot.

Conditions: The symptom is observed when there is a tunnel (Ethernet over MPLS over GRE over IPSec) between PE1 and PE2 and following a reload and when tunnel protection is configured.

Workaround: There is no workaround.

- CSCtl50815

Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

```
%OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
Non-OER, OOP Reason <reason>
```

Conditions: The symptom is observed under the following conditions:

- Use ECMP.
- Use **mode monitor passive**.

Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl52854

Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

Conditions: This symptom is observed when a multicast server is connected to an EHWIC L2 interface.

Workaround: Connect the multicast server to an on-board gig interface.

- CSCtl54975

Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

Conditions: Unknown.

Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl55502

Symptoms: Any parser command with a pipe option used in an HTTP URL is not working properly and giving the help option instead of the actual output.

Conditions: The symptom is observed when a parser command uses a pipe option in an HTTP URL (for example, <http://<ipadd>/level/15/exec/show/runn//i/http/CR>).

Workaround: There is no workaround.

- CSCtl74521

Symptoms: Crackling voice is heard on the PSTN rx side.

Conditions: This symptom occurs under the following conditions:

- RTP comes from Multilink interface. There is no audible crackling in the RTP stream.
- If used, codec g711ulaw with packetization > 80 bytes.

Workaround: Set codec packetization to 80 bytes on dial-peer or voice-class codec.

- CSCtl82517

Symptoms: For the Cisco ME3600 and Cisco ME3800, the following licensing errors are seen, leading to license manager failure at bootup:

```
%SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0). -Process=
"Init", ipl= 4, pid=
```

Conditions: This symptom is seen when a Cisco ME3600 or Cisco ME3800 license-based image is loaded off mcp_dev_nile.

Workaround: Use whales-universal-mz.

- CSCtl90341

Symptoms: A router crashes due to an NHRP stack overflow.

Conditions: This symptom occurs very inconsistently.

Workaround: There is no workaround.

- CSCtn04277

Symptoms: Time-based WRED does not work.

Conditions: The symptom is observed when time-based WRED is used in Cisco IOS Release 15.1(3)T.

Workaround: There is no workaround.

- CSCtn04357

Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

```
vlan configuration 161 ip flow monitor flowmonitor1 in ip flow monitor flowmonitor1
input
```

Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

Workaround 1: Remove the flow monitor configuration.

Workaround 2: Use netflow-v9 export protocol.

Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn08673

Symptoms: A Cisco device crashes with tracebacks:

```
08:56:31 gmt Fri Jan 14 2011: Unexpected exception to CPU: vector D, PC = 0x3CD7565
%Traceback= 3CD7565 29D255AC 3D5602E 3D3A510 3D69BC2 3CC49C8 3CC2266 3CCD42B 3CCC96D
```

Conditions: This symptom is observed on a Cisco 3900 running Cisco IOS Release 15.1(1)T1.

Workaround: There is no workaround.

- CSCtn10507

Symptoms: Tracebacks at fw_dp_base_process_new_pak & fw_dp_state_object_init_obj IPv6 routing and mediatrace do not come up.

Conditions: This symptom is observed when FW with self zones is configured on the router.

Workaround: There is no workaround.

- CSCtn12119

Symptoms: There is no change in functionality or behavior from a user perspective. This DDTs brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn18784

Symptoms: Interface Tunnel 0 constantly sends high-bandwidth alarms.

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn21198

Symptoms: Placing fax calls through c5510 DSP (NM-HDV2, etc) using Voice over Frame Relay (VoFR) may trigger UNSUPPORTED CODEC messages on the console and possibly a WatchDog Timeout.

Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T and Release 15.1(4)M.

Workaround: Use Voice over IP (VoIP) instead of VoFR, or use an older IOS release.

- CSCtn21501

Symptoms: A Cisco 2900 series router with switch modules (such as HWIC-4ESW-POE or HWIC-D-9ESW-POE) does not respond to SNMP queries on the BRIDGE-MIB.

Conditions: The symptom is observed on a Cisco 2900 series router (with switch modules) that is running Cisco IOS Release 15.x.

Workaround: There is no workaround.

Further Problem Description: This issue is similar to CSCsb46470.

- CSCtn31333

Symptoms: High CPU utilization is observed on the Cisco CMTS router due to the Net Background process.

Conditions: This symptom is observed on a router used for L2TP network server (LNS) with an L2TP application.

- Workaround: There is no workaround.
- CSCtn40571

Symptoms: Issuing the **crypto pki server name rollover cancel** command can result in multiple rollover certificates installed on Sub-CA router.

Conditions: This symptom is seen when the rollover certificate is already installed.

Workaround:

 - Copy startup-configuration from router.
 - Remove the older rollover certificate from configuration under the **crypto pki cert chain ca** command.
 - Copy the new configuration back to startup-configuration and reload the router.
 - CSCtn43589

Symptoms: A crash is observed at process_run_degraded_or_crash.

Conditions: The symptom is observed when SNMP bulkstat has been configured for periodic MIB collection.

Workaround: There is no workaround.
 - CSCtn47119

Symptoms: Router crashes when sending IPv6 ping packets.

Conditions: The symptom is observed when a ping is issued with a packet size of more than 1500 bytes.

Workaround: There is no workaround.
 - CSCtn58128

Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

Workaround: Ensure “no logging console” is configured.
 - CSCtn59075

Symptoms: A router may crash.

Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.

Workaround: There is no workaround.
 - CSCtn65060

Symptoms: A Cisco device crashes.

Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”

Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.
 - CSCtn68117

Symptoms: Session command does not work on Cisco C3K series routers that have become the master after a mastership change.

Conditions: This symptom is seen when fail-over to slave occurs.

Workaround: There is no workaround.

- CSCtn79475

Symptoms: A Cisco router reloads often due to stack overflow under some traffic conditions.

Conditions: This symptom is observed when calls resulting in VOIP RTP media loop are seen.

Workaround: There is no workaround.

- CSCtn93891

Symptoms: Multicast traffic is getting blocked.

Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

Workaround: There is no workaround.

- CSCtn97267

Symptoms: There is a router crash in the URLF code using Websense.

Conditions: The symptom is observed on a Cisco ISR G2 during normal operation. It is caused by long URLs overwriting the end of a fixed length buffer.

Workaround: There is no workaround.

- CSCto00796

Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)

Workaround: Soft clear the peer that missed getting the RT.

- CSCto02712

Symptoms: A router that is running Cisco IOS Release 15.1(4)M1 with “proxy-arp” enabled will incorrectly reply to duplicate address detection ARP requests sourced from end devices.

Some end devices will send an ARP request for their assigned IP to check for duplicate address detection per RFC5227. When this occurs the router should ignore this ARP request. With this issue, the router will respond to the request, which triggers the duplicate address detection on the end device and breaks connectivity between the router and end device.

Conditions: The symptom is observed with the following conditions:

- “proxy-arp” is enabled on client facing Layer-3 interface.
- end device sends a “duplicate address detection” ARP request on its local subnet.

Workaround 1: Configure **no ip proxy arp** on client-facing interface.

Workaround 2: Disable “duplicate address detection” on the end device.

- CSCto05108

Symptoms: A Cisco 7206 with VSA card is used as a GETVPN GM. After some time of operation, the router prints VSA-related traceback and completely stops encrypting/decrypting any traffic:

```
%008720: Feb 24 11:11:01.674 GMT+5: VSA shim: crypto_ike_encrypt_callback ctx_next
NULL -Traceback= 0x1BF4364z 0x3D38AE4z 0x3D007FCz 0x3CFA77Cz 0x3CFE108z 0x15829FCz
0x15857ACz 0x1584800z 0x15822C8z 0x5580000z 0x1584E78z 0x1582384z 0x3D00DD8z
0x3D00A64z 0x3D3852Cz 0x3D411B0z
```

After that, all encrypted traffic is dropped. Crypto debugs (debug crypto isakmp, etc) do not produce any messages. The only way to recover is to reboot the router.

Conditions: This symptom is observed on a Cisco 7206 where a VSA card is used as a GETVPN GM and running Cisco IOS Release 15.0(1)M4 or Release 12.4(24)T3.

Workaround: Disable encryption.

- CSCto08135

Symptoms: When a deny statement is added as the first ACL, the message gets dropped.

Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.

Workaround: Turn off the VSA, and go back to software encryption.

- CSCto10485

Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the %CRYPVO-4-PKT-REPLAY drops as shown in the syslog.

Conditions: This issue typically occurs during high traffic load conditions.

Workaround: There is no workaround.

- CSCto14518

Symptoms: The command **show memory debug leak** may crash a router.

Conditions: The symptom is observed when using the command **show memory debug leak**.

Workaround: There is no workaround.

- CSCto15361

Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto34844

Symptoms: The Cisco 891 may perform lower than the older generation Cisco 1812 platform.

Conditions: This symptom occurs when Ethernet traffic using the VLAN tag is encapsulated inside the L2TPv3 tunnel.

Workaround: There is no workaround.

- CSCto39885

Symptoms: A router crashes.

Conditions: gcid and callmon is turned on.

Workaround: There is no workaround.

- CSCto41165

Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit/deny** command, and then the **no ip extcommunity-list 55 permit/deny** command.

Conditions: This symptom occurs when the standby router is configured.

Workaround: There is no workaround.

- CSCto41173

Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.

Conditions: This symptom is observed with a platform that acts as an H323 gateway and runs Cisco IOS Release 15.1(3)T.

Workaround: Revert to Cisco IOS Release 12.4(20)T.

- CSCto43683

Symptoms: Suspended service policy is not re-enabled when an MFR bundle link comes up.

Conditions: The symptom is observed when the service policy is attached to MFR DLCI.

Workaround: There is no workaround.

- CSCto48060

Symptoms: A Cisco 3900 series router may crash with the following error:

```
Unexpected exception to CPU: vector 1400
```

Conditions: The symptom is observed when the router is configured as a voice gateway using H323 and H245 and connected to CUCM. If CUCM is sending a MultiMediaSystemControl messages with no entry, the router may crash.

Workaround: There is no workaround.

- CSCto60047

Symptoms: A crash occurs either due to a chunk corruption or at ssh_send_queue_data.

Conditions: This symptom occurs under the following conditions:

- An SSH session exists between two routers.
- The **show tech** command is issued and then aborted.

Workaround: There is no workaround.

- CSCto63268

Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

Workaround: Remove the EVM or disable DSP sharing.

- CSCto65352

Symptoms: A system crashes randomly when an Apex module is in the system.

Conditions: The system crashes under normal conditions.

Workaround: There is no workaround.

- CSCto72629

Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto81701

Symptoms: The PfR MC and BR sessions flap.

Conditions: The symptom is observed with a scale of more than 800 learned TCs.

Workaround: Use the following configuration:

```
pfr master
  keepalive 1000
```

- CSCto81916

Symptoms: Voice gateway crashes due to insufficient free memory.

Conditions: The symptom is observed when the copy feature is used in a voice class SIP profile similar to the example below:

```
voice class sip-profiles 500
  request INVITE peer-header sip Remote-Party-ID copy ":(.*)@" u01
  request INVITE sip-header From modify "From: \"anonymous\" <(.*):(.*)
@" "From: \"\u01\" <\1:\u01@"
!
```

In this case, a memory leak occurs and depletes all the free memory causing the router to crash.

Workaround: There is no workaround.

- CSCto85479

Symptoms: Spanning Tree Protocol (STP) failure on EHWIC-4ESG.

Conditions: The symptom is observed on a Cisco 3945 chassis that is running the c3900-universalk9-mz.SPA.151-4.M.bin image. Interfaces gi0/3/0-1 are on EHWIC-4ESG card.

Workaround: There is no workaround.

- CSCto88393

Symptoms: CPU hogs are observed on a master controller:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0),process =
OER Master Controller.
```

Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

Workaround: There is no workaround.

- CSCto99343

Symptoms: Linecards do not forward packets which causes a failure on the neighborship.

Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.

Workaround: There is no workaround.

- CSCto99523

Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

Conditions: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

Workaround: There is no workaround.

- CSCtq04117

Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running.

Conditions: This symptom occurs under the following conditions:

1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

Workaround: Use the **clear ip route vrf x *** command.

- CSCtq05004

Symptoms: A dialer loses its IP address sporadically.

- “show interface atm x” will record output drops during the issue.

```
ATM0 is up, line protocol is up
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 31956 <<
Incrementing during the issue
```

- “show interface queueing atm0.1” (hidden command) will show as follows:

```
Interface ATM0 VC 8/35 Queueing strategy: fifo Output queue 40/40, 31956 drops per
VC << Incrementing during the issue
```

- During the issue, if “debug ppp negotiation” is on, we will see the following:

```
PPP: Missed 5 keepalives, taking LCP down
PPP DISC: Missed too many keepalives
```

- There will be no ATM (physical interface) flap in this case (during the issue).
- shut/no shut on the ATM interface does not help.

Conditions: No conditions so far. The behavior is sporadic.

Workaround: Reload.

- CSCtq05636

Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg. For example:

Received:

```
INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
```

Sent:

```
INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
```

In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq06538

Symptoms: RP crashes due to bad chunk in MallocLite.

Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

```
LOCAL_PREF Header AttributeFlags Optional: 0b0 Transitive: 0b1 Partial: 0b0
ExtendedLength: 0b0 Unused: 0b0 0b0 0b0 0b0 TypeCode: 0x05 Length: 0x01 <----- should
be 0x04 instead Value: 0xff 0xff 0xff 0xff NetworkLayerReachabilityInfo: 0x08 0x0a
<snip>
```

Workaround: There is no workaround.

- CSCtq07413

Symptoms: A hardware crypto engine may fail to decrypt packets. An “invalid parameter” error is seen after decryption. Software encryption works fine.

Conditions: This symptom is observed in Cisco IOS Release 12.4.15T6.

Workaround: Use software encryption.

- CSCtq10356

Symptoms: When video is enabled under a call manager profile, the Zone-Based Firewall SIP inspection engine will not create the RTP pinhole for voice.

Conditions: This symptom is observed when video is enabled under the phone profile.

Workaround: Disable video under the phone profile; the two options to disable are “Cisco Camera” and “Video Capabilities.”

- CSCtq10524

Symptoms: A Cisco device may crash.

Conditions: This symptom is observed when more than the recommended number of Mediatrace sessions (>255) is applied to one interface.

Workaround: Keep the number of Mediatrace sessions below the recommended maximum per interface.

- CSCtq10684

Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

Conditions: This symptom occurs when tunnel flap is observed before the crash.

Workaround: A possible workaround is to reload the box.

- CSCtq12007

Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less severe; you may see one every other packet drop, until the next rekey or tunnel reset.

Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq15247

Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

For example:

```
LAC1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
LAC1(config)#interface virtual-ppp1
LAC1(config-if)#no pseudowire
LAC1(config-if)#exit
LAC1(config)#no interface virtual-ppp1
```

- CSCtq18068

Symptoms: An “autoqos:error” is seen when configuring auto QoS VoIP.

Conditions: This symptom is observed in Cisco IOS Release 15.2(1)T.

Workaround: There is no workaround.

- CSCtq21234

Symptoms: Label is not freed.

Conditions: The symptom is observed after shutting down the link.

Workaround: There is no workaround.

- CSCtq21785

Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(2)S may crash upon performing a CRL check on an invalid certificate.

Conditions: The conditions are unknown.

Workaround: Turning off CRL check should stop the crash. It should be configured as:

“revocation-check none”

This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq26892

Symptoms: CUBE crashes @ sipSPI_ipip_IsHdrInHeaderList.

Conditions: This symptom is observed with a PRACK-NO PRACK configuration on Cisco IOS Release 15.2(1)T.

Workaround: There is no workaround.

- CSCtq28392

Symptoms: A Cisco 860 router crashes.

Conditions: The symptom is observed on a Cisco 860 router when applying tunnel protection on the tunnel interface.

Workaround: Use a crypto map configuration.

- CSCtq28732

Symptoms: Memory leak is observed when device is configured **parameter-map type inspectglobal**.

Conditions: Device is configured with **parameter-map type inspect global**.

See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfbw>

Workaround: There is no workaround.

- CSCtq29554

Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

Workaround: Reload the failing line card to recover it.

- CSCtq30686

Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.

Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.

Workaround: There is no workaround.

- CSCtq33102

Symptoms: A Cisco router that is acting as an RA crashes in an SDP environment with CVO setup.

Conditions: This symptom occurs during CVO enrollment request.

Workaround: There is no workaround.

- CSCtq36153

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

- Memory Leak Associated with Crafted IP Packets
- Memory Leak in HTTP Inspection
- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfbw>

- CSCtq49325

Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq55173

Symptoms: A device that is configured with NAT crashes. SIP appears to be translated through NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezybn** command is entered.

Workaround: There is no workaround.

- CSCtq56727

Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash.

The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP, and other processes.

“sh proc mem sorted” shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

Conditions: This symptom occurs when the SIP trunk in Unified Communications Manager pointing to the gateway is configured with a DTMF signaling type of “no preference” and the SIP gateway is configured with DTMF relay as sip-kpml.

Workaround: There are two workarounds:

1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”

Recovery: In order to recover from the crash, you must reload the gateway router.

- CSCtq58383

Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq61850

Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

Workaround: There is no workaround.

- CSCtq62322

Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).

Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.

Workaround: There is no workaround.

- CSCtq62759

Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq64034

Symptoms: NAT does not send gratuitous ARP for a translated address when an interface comes up.

Conditions: The symptom is observed when an alias (translated address) is created with the interface (whose IP address is in the same subnet as the alias entry) is in shut down state.

Workaround: Perform an admin shut/no shut on the interface with an IP address in the same subnet as the alias entry.

- CSCtq67959

Symptoms: Tracebacks are seen on a Cisco 7200 series router.

Conditions: The issue seen while testing the IPv6 OSPF feature.

Workaround: There is no workaround.

- CSCtq69083

Symptoms: Nested IPsec tunnel with outer tunnel GRE and inner tunnel VTI/GRE is not working.

Conditions: The symptom is observed with the v150-1.M4.6 image.

Workaround: There is no workaround.

- CSCtq75008

Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

Conditions:

- The Cisco 7206 VXR works as a server for L2TP over IPsec.
- Encryption is done using C7200-VSA.
- More than two clients are connected.

If client sessions are kept up for about a day, the router crashes.

Workaround: There is no workaround.

- CSCtq76005

Symptoms: Configuring “atm route-brige ip” on MPLS-enabled ATM interface makes router punt all incoming MPLS packets to CPU.

Conditions: The symptom is observed when RBE is configured on a MPLS-enabled ATM interface.

Workaround: Remove RBE.

- CSCtq77274

Symptoms: FXS phones are not recognized as SCCP endpoints.

Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

Workaround: There is no workaround.

- CSCtq77363

Symptoms: License images are not working properly.

Conditions: This symptom is seen when the license image is loaded. There is a traceback due to access of uninitialized variables.

Workaround: There are no workarounds.

- CSCtq78217

Symptoms: A router crashes with the following information:

System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ

Conditions: The symptom is observed with CUBE + SIP.

Workaround: There is no workaround.

- CSCtq80648

Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

For example:

```
interface Ethernet1/0
  vrf forwarding vpn1
  ipv6 address 1::1/64
!
router bgp 65000
  address-family ipv6 vrf vpn1
    neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq80858

Symptoms: A router crashes randomly at various decodes.

Conditions: This symptom is observed when MACE and IP SLA TCP-based probes are configured.

Workaround: There is no workaround.

- CSCtq84635

Symptoms: Trunk DN's can act as if busy (such as by triggering CFB) even though they have no calls and show commands for ephone-dns or ports report nothing unusual.

Conditions: This symptom occurs in Cisco IOS Release 15.0(1)M after heavy use; it is believed not to occur in Cisco IOS Release 12.4(20)T or prior releases.

Workaround: Delete and re-add trunk DN's.

- CSCtq85728

Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.

Workaround: There is no workaround.

- CSCtq86500

Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

Workaround: Disable VSA and use software encryption.

- CSCtq86515

Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq90577

Symptoms: A router crashes when removing Netflow.

Conditions: The symptom is observed when removing Netflow.

Workaround: There is no workaround.

- CSCtq91176

Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtq92182

Symptoms: An eBGP session is not established.

Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq92940

Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtq96329

Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

Conditions: This symptom can happen only when bgp deterministic-med is configured.

The following releases are impacted:

- Cisco IOS Release 15.0(1)S4
- Cisco IOS Release 15.1(2)T4
- Cisco IOS Release 15.1(3)S
- Cisco IOS Release 15.2(1)T

Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr09251

Symptoms: Continuous alignment errors and performance degradation in throughput of MS RPC traffic through the ZBFW.

Conditions: The symptom is observed when inspecting MS RPC traffic through the ZBFW on a Cisco 2911 router that is running Cisco IOS Release 15.1(4)M.

Workaround: There is no workaround.

- CSCtr11620

Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

Conditions: This symptom is observed when a Cisco 2911 is used.

Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr13172

Symptoms: The **config replace** command crashes the router.

Conditions: The symptom is observed when close to the maximum number of mediatrace and performance monitoring policies along with DMVPN are configured on the router and the target configuration contains none of these elements.

Workaround: Uninstall the mediatrace and performance monitor policies prior to replacing the configuration.

- CSCtr14763

Symptoms: A BFD session is always up, although the link protocol is down.

Conditions: First the BFD session is up between the routers. After the VLAN is changed on the switch between the routers, the BFD peer is not reachable but the BFD sessions are always up.

Workaround: There is no workaround.

- CSCtr15891

Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

Workaround: There is no workaround.

- CSCtr18559

Symptoms: An unallocated/unassigned number is received from PBX but as a response, a network congestion message is sent back. Gateway rejects call with 4# when actually its supposed to send a 7#.

Conditions: The issue occurs only when the country Brazil is configured. When country is set to "itu", then a 5# is sent which is correct for an unallocated/unassigned number. Follow this link to track cause code to CAs mapping sbased on selection of countries:

<http://www.pulsewan.com/data101/r2mfc.pd>

Workaround: There is no workaround.

- CSCtr20908

Symptoms: A spurious access will occur on platforms that detect spurious accesses. A crash will occur on platforms that do not detect spurious accesses such as the Cisco ASR 1000, Cisco 3900 and 3900e.

Conditions: The issue occurs when running the **show run all** command and when WEBVPN configurations are present.

Workaround: Use the Cisco IOS 15.1(3)T train.

- CSCtr25821

Symptoms: A Cisco 800 series router crashes with **isdn leased-line bri0 128** command:

```
Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310
```

Conditions: The symptom is observed with the **isdn leased-line bri0 128** command.

Workaround: The issue does not occur if there is no cable that connects to the BRI interface. Disconnect the cable from the BRI interface while **isdn leased-line bri0 128** is configured.

- CSCtr28857

A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp>

- CSCtr29338

Symptoms: A router crashes.

Conditions: The symptom is observed after an %ISDN-6-DISCONNECT message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.

Workaround: There is no workaround.

- CSCtr44686

Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
  class type inspect smtp SMTP_L7_C1
    reset
policy-map type inspect smtp SMTP_L7_P2
  class type inspect smtp SMTP_L7_C2A
    reset
  class type inspect smtp SMTP_L7_C2B
    reset
```

Conditions: The symptom is observed with the above maps.

Workaround: Replace “reset” with “log”.

- CSCtr45608

Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr45633

Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.

Conditions: The symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.

Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address-family”.

- CSCtr49064

The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh>

- CSCtr51786

Symptoms: The command **passive-interface** for a VNET auto-created subinterface x/y.z may remove the derived interface configuration command **ip ospf process id area number**. Consequently, putting back **no passive-interface** command will not form the lost OSPF ADJ.

Conditions: The symptom is observed only with interfaces associated with the OSPF process using the command **ip ospf vnet area number**.

Workaround: Associate the interface with the OSPF process using a network statement or using the interface command **ip ospf process id area number**.

Further Problem Description: Interfaces associated with a process using a network statement under “router ospf” or interfaces configured with the command **ip ospf process id area number** are not affected.

- CSCtr54269

Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr58140

Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

Workaround: There is no workaround.

- CSCtr71465

Symptoms: A router crashes at `ipv4fib_les_switch_fastswitching_compat` while booting.

Conditions: The symptom is observed on a Cisco 888E router that is running Cisco IOS interim Release 15.1(2)T1.1 or later.

Workaround: There is no workaround.

- CSCtr89322

Symptoms: NME-RVPN module is not recognized by a Cisco 3900e router.

Conditions: The symptom is observed with a Cisco 3900e router.

Workaround: There is no workaround.

- CSCtr91106

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai>

- CSCtr94887

Symptoms: Using MRCP v1, VXML script with ASR operation will always receive noinput event.

Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T.

Workaround: There is no workaround.

- CSCtr97640

Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

Conditions: None.

Workaround: None--Physically securing the router is important.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.9/1.8:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C>

CVE ID CVE-2011-3289 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts20102

Symptoms: NVRAM may lose or corrupt after router comes up.

Conditions: The symptom is observed during stress testing.

Workaround: Use the **wr erase** and then the **wr memory** commands if NVRAM corruption occurs.

- CSCts28462

Symptoms: snmp-server host 1.2.3.4 traps version 2c public nhrp is reported as snmp-server host 1.2.3.4 traps version 2c public ds3.

Conditions: Unknown.

Workaround: There is no workaround.

- CSCts33952

Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

Workaround: There is no workaround.

- CSCts39535

Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

Resolved Caveats—Cisco IOS Release 15.1(4)M1

Cisco IOS Release 15.1(4)M1 is a rebuild release for Cisco IOS Release 15.1(4)M. The caveats in this section are resolved in Cisco IOS Release 15.1(4)M1 but may be open in previous Cisco IOS releases.

- CSCs118054

Symptoms: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, not after failed logins.

Symptoms: This symptom occurs on a router running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCso33003

Symptoms: If a child policy is attached to a parent policy twice, the router will reload if the child policy configuration is removed.

Conditions: The parent policy needs to be attached to the target interface.

Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCtc11266

Symptoms: The router undergoes a bus error crash. Before the crash, the following error messages are displayed:

```
%SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
%SYS-4-SNMP_WRITENET: SNMP WriteNet request.
%ALIGN-1-FATAL: Illegal access to a low address
```

Conditions: This symptom is observed on a router running Cisco IOS Release 12.4(22)T1 that is used as a zone-based firewall with no routing and VPN configured.

```
outside---ASA firewall-----gig-IOS firewall-gig-----inside network
```

Workaround: There is no workaround.

- CSCtd23069

Symptoms: A crash occurs because of a SegV exception after configuring the **ip virtual-reassembly** command.

Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd90030

Symptoms: A Cisco 2851 router may crash with a bus error.

Conditions: This symptom is observed when the function calls involve Session Initiation Protocol (SIP) and are possibly related to an IPCC server. This issue is seen with Cisco IOS Release 12.4(24)T1 or Cisco IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtf39056

Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.

Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
#####
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
#####
```

- CSCtf71673

Symptoms: A Cisco 10000 series router shows a PRE crash due to memory-corruption with block overrun.

Conditions: This symptom is seen when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

Workaround: There is no workaround.

- CSCth20018

Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, **no interface g0/0.100** or **no interface atm0/0.100**), may sometimes crash the system.

Conditions: This symptom occurs during basic configuration.

Workaround: Do not unconfigure a subinterface.

- CSCti53157

Symptoms: If the console speed is changed, sometimes due to a change in speed, the characters are treated as break characters by Cisco IOS, and the system goes to ROMmon.

Conditions: This symptom is seen if the console speed is changed.

Workaround: There is no workaround. This caveat is Closed.

- CSCti64685
Symptoms: User may not be able to configure SLA MPLS configuration.
Conditions: This symptom occurs when the router is booted up and may be random.
Workaround: There is no workaround.
- CSCtj15798
Symptoms: Some modems in PVDM2-xxDM module are marked as BAD after running clean for few days. The **show modem** command will report a “B” in front of the modem (“B - Modem is marked bad and cannot be used for taking calls”).
Conditions: The symptom is observed with the PVDM2-xxDM module.
Workaround: Reloading the router gives a few more days of clean connections before the issue is seen again.
- CSCtj21045
Symptoms: Header compression decodes RTP timestamp incorrectly.
Conditions: This issue occurs mainly with IPHC format compression interacting with older Cisco IOS releases.
Workaround: Use IETF format compression.
- CSCtj23189
Symptoms: Packet drops occur on low-rate bandwidth guarantee classes even if the offered rate is less than the guaranteed rate.
Conditions: This symptom occurs only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with three classes: one with 16kbps, the second one with 1Mbps, and the third one with 99Mbps.
Workaround: There is no workaround.
- CSCtj46670
Symptoms: IPCP cannot be completed after the dialer interface is moved out of standby mode. CONFREJ is seen while negotiating IPCP.
Conditions: The symptom is observed when a dialer interface has moved out from standby mode.
Workaround: Reload the router.
- CSCtj57173
Symptoms: The Cisco IOS Software crashes when processing a specially crafted DNS reply packet.
Conditions: This symptom occurs when the router is configured for DNS server operations via the **ip dns server** command. This issue affects all versions of the Cisco IOS Software prior to first fixed software.
Workaround: Disable the IP Name server functionality on the Cisco IOS Software.
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5:
<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C>
CVE ID CVE-2011-0958 has been assigned to document this issue.
Additional information on Cisco’s security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtj78966

Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

Conditions: This symptom occurs when the IKEv2 SA DB WAVL tree is getting corrupted if you fail to insert the SA due to some error, for example, PSH duplication.

Workaround: There is no workaround.

- CSCtj84234

Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

```
route-map <RM name>
  match ip address <acl>
  set ip next-hop <NH1> <NH2>
```

Workaround: There is no workaround.

- CSCtj87846

Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

Workaround: Do a shut/no shut on PfR master or PfR border.

- CSCtj91149

Symptoms: A delay of approximately 30 seconds is observed in a dynamic xconnect-based ISG session that comes up on standby, after it is up on active.

Conditions: This symptom occurs on switchover.

Workaround: There is no workaround.

- CSCtj91419

Symptoms: When the reset push button is pressed and the default golden Cisco IOS image (*.default) is not present in flash, the push button status is not shown in “show platform boot-record” after Cisco IOS boots up.

Conditions: This symptom is seen when the reset push button is pressed when ROMmon boots up, and the default golden Cisco IOS image should not be present in the flash.

Workaround: Make sure .default Cisco IOS image is present in the flash whenever the reset push button is pressed. This caveat is Closed.

- CSCtj94510

Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), with one IKE session per VRF and four SA dual per session, a crash happens on Crypto_SS_process.

Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), with one IKE session per VRF and four SA dual per session.

Workaround: There is no workaround.

- CSCtk09402

Symptoms: Bandwidth class may not get the correct bandwidth when policy map is configured.

Conditions: This problem is seen on Cisco 800 series routers (Cisco 886W, Cisco 887W) on the DSL interface.

Workaround: Fine tune using the **queue-limit** command. This will ensure the total bandwidth is available for the desired stream of traffic. Default queue-limit is 64 packets. Increasing it to 128 packets should solve the problem. This caveat is Closed.

- CSCtk18330

Symptoms: MSCHAPv2 auth fails when matching the user/password pair is configured.

Conditions: This symptom is observed when matching the user/password pair is configured.

Workaround: There is no workaround.

- CSCtk53674

Symptoms: An rtr running Cisco IOS Release 12.4(15)T14 and Cisco IOS Release 15.0M will crash when SNMPv3 configuration is removed.

Conditions: This symptom occurs when the running configuration contains the following depending on the Cisco IOS Release:

Cisco IOS Release 12.4(15)T14

```
snmp-server user QoSqosuser1 QoSqosgroup v3 enc auth sha <DIGEST>
priv aes 128 qosQ00!priv acc SNMP
```

Cisco IOS Release 15.0(1)M4

```
snmp-server user QoSqosuser1 QoSqosgroup v3 enc auth sha <DIGEST>
priv aes 128 qosQ00!priv acc SNMP
```

When you remove the above configuration using the **no snmp-server user** command, the rtr crashes.

Workaround: There is no workaround.

- CSCtk58027

Symptoms: The router crashes with the ip sla icmp jitter operation.

Conditions: This symptom is observed when recreate steps have the ip sla icmp jitter operation with more number of packets running along with voice and data traffic running. When the status of the ip sla is OK, enter the **no ip sla schedule** command, and then enter the **no ip sla operation-number** command.

Workaround: There is no workaround.

- CSCtk67073

The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla>.

- CSCtk67709

Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

```
ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432-k9.pkg
```

SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive

Conditions: This symptom is observed with AnyConnect 3.0.

Workaround: There is no workaround.

- CSCtk67934

Symptoms: A Cisco router is forced to reload after a few days of encryption and decryption while processing high traffic.

Conditions: This symptom is observed when VSA is enabled as a hardware crypto engine used for processing both firewall and encryption/decryption on the same interface.

Workaround: Switch from VSA HW crypto engine to either SW crypto engine or VAM2+ HW crypto engine.

- CSCtk74660

Symptoms: The Network Time Protocol (NTP) tries to resync after the server clock changes its time and after the NTP falls back to the local clock.

Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

Workaround: There is no workaround.

- CSCtl04432

Symptoms: The **show power inline fastethernet** command will show the interfaces that do not support power over ethernet. On Cisco 88xW platforms, PoE is supported only on FE0 and FE1.

Conditions: This symptom happens on Cisco 88x series routers that are running Cisco IOS Release 15.1(4)M1.

Workaround: There is no workaround. This caveat is Closed.

- CSCtl20993

Symptoms: The router crashes during IPSec rekey.

Conditions: The conditions for this crash are currently unknown.

Workaround: There is no workaround.

- CSCtl43156

Symptoms: When using a BVI interface configured for IPv6 on a Cisco ISR-G2 series router, IPv6 neighbors are never discovered over the BVI. Neighbors will never be seen in the **show ipv6 neighbors** output and all traffic to/through the BVI will fail.

Conditions: This symptom occurs when IPv6 is configured on Cisco ISR-G2 router images running on the “datak9” package.

Workaround: Use the “uck9” technology package, where the IPv6 feature is already present.

- CSCtl44103

Symptoms: The Cisco 3945 router that is running Cisco IOS Release 15.1(3)T has a zone-based firewall configured.

Conditions: This symptom occurs when using any of the following three debug commands:

- **debug policy-map type inspect events**
- **debug policy-firewall events**
- **debug ip inspect events**

This symptom crashes the router immediately.

Workaround: There is no workaround.

- CSCtl45307

Symptoms: BOOTP requests are not forwarded by the router.

Conditions: This symptom occurs with BOOTP requests.

Workaround: There is no workaround.

- CSCtl45684

Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

```
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726
ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
```

Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.

Workaround: There is no workaround.

- CSCtl53899

Symptoms: SIP to SIP calls through CUBE may cause memory corruption when resource priority passthrough is enabled on the dial peers.

Conditions: This symptom is observed on CUBE with Cisco IOS Release 15.1(3)T, where the following was configured under the SIP dial peers:

```
voice-class sip resource priority mode passthrough
```

Workaround: Disable memory lite allocations using the **no memory lite** command. This will increase the size of memory allocations, so be careful when using it on a device with high memory utilization.

- CSCtl54415

Symptoms: A Cisco router or switch may reload.

Conditions: This symptom is experienced on multiple platforms when single-connection timeout is configured under an aaa group server, and there is no TACACS key configured:

```
aaa group server tacacs+ <NAME>
  server-private x.x.x.x single-connection timeout 2
  server-private x.x.x.x single-connection timeout 2
  ip tacacs source-interface Loopback0
(no tacacs-server key configured)
```

Workaround: Either configure the correct matching key or do not configure single-connection timeout.

- CSCtl58005

Symptoms: Accounting delay start is sent before any NCP has been negotiated, with “aaa accounting delay-start” configured. According to PRD, accounting start should not be sent until first NCP has been negotiated.

Conditions: This symptom occurs when “aaa accounting delay-start” is configured.

Workaround: There is no workaround.

- CSCtl70143

Symptoms: LAC does not forward a PPP CHAP-SUCCESS message from LNS to the client sometimes.

Conditions: This symptom is seen when T1/PRI is used between the client and LAC.

Workaround: There is no workaround.

- CSCtl73914

Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

Conditions: This symptom is observed if the P-Associated-URI of the 200 Ok response contains any special characters (!*!) in Tel URI Parsing.

Workaround: There is no workaround.

- CSCtl78285

Symptoms: In a VRF configuration, rd cannot be added after deleting rd configuration once:

```
A-SUP5-6509E#sho run | be vrf
ip vrf CUST1
    rd 1:1
    route-target export 1:1
    route-target import 1:1
    mdt default 239.39.39.39
```

```
A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#no rd 1:1
% "rd 1:1" for VRF CUST1 scheduled for deletion
```

Wait and try to add rd again (for more than 2 hours).

```
A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#rd 1:1
% Deletion of "rd" in progress; wait for it to complete
A-SUP5-6509E(config-vrf)#
```

Conditions: This symptom is seen in a VRF configuration with rd.

Workaround: Remove the VRF configuration and add it again.

- CSCtl79627

Symptoms: The Cisco 891W router stops accepting new connections via SSL VPN, SSH, Telnet, and HTTP due to a memory leak, which results in memory depletion on the router.

Conditions: This symptom is observed on a Cisco 891W router running the latest Cisco IOS Release 15.1(3)T.

Workaround: There is no workaround.

- CSCtl81133

Symptoms: A Cisco CUBE router using SIP TLS will crash if the outgoing SIP TLS connection attempts from CUBE to another endpoint do not successfully negotiate.

Conditions: This symptom occurs on CUBE running Cisco IOS Release 15.1(3)T, using SIP TLS, and SIP options keepalive between CUBE and a third-party SIP device. Outgoing TCP connections from CUBE are accepted by the third-party device, but then closed shortly following the TLS client hello message from CUBE.

Workaround: There is no workaround.

- CSCtl94813

Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analogue phone on the VG224 attends a conference bridge. It causes one-way audio.

- When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen.
- For the same call, the PCM trace shows no audio in the RIN stream.

Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

```
*Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx:
Got RX stats
Packet details:
Packet Length=188, Channel Id=1, Packet Id=200
RX Packets=0: Signaling=0, ComfortNoise=0
Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms)
Packet Counts: OoSequence=0, Bad header=0, Late=0, Early=0Receive
inactive duration=129(ms)
```

Workaround: Downgrade the Cisco IOS to Cisco IOS Release 12.4(4)T8.

- CSCtl95752

Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.

Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.

Workaround: There is no workaround.

- CSCtn00405

Symptoms: A Cisco router may crash when “isdn test call” is run.

Conditions: This symptom has been experienced on multiple IOS versions, including Cisco IOS Release 12.4(15)10, 12.4(24)T4, and 15.0(1)M4.

Workaround: There is no workaround.

- CSCtn02428

Symptoms: In “show mem alloc tot”, the top allocators are “CCE DP SIP Tx” and “FW SIP SESS WRAP”:

```
Allocator PC Summary for: Processor
Displayed first 2048 Allocator PCs only
```

PC	Total	Count	Name
0x63DE1B14	163317100	10236	CCE DP SIP Tx
0x64713A20	23784460	241386	FW SIP SESS WRAP
...			

Conditions: This symptom is observed during ZBF + SIP traffic.

Workaround: There is no workaround.

- CSCtn04686

Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unplugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.

Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.

Workaround: Unplug/plug the cables.

- CSCtn08208

Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.

Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.

Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.

- CSCtn15317

Symptoms: Traffic on MPLS VPN is dropped. When you check LFIB information on the P router, the entry has an instruction to TAG all packets that are destined to the PE router instead of a POP instruction which is expected on a directly connected P.

Conditions: This symptom occurs with the following conditions:

- The ISIS protocol is running as IGP on MPLS infrastructure.
- ISIS on the PE router is summarizing network that includes BGP vpnv4 update-source.
- The P router is running an MFI-based image.

Workaround 1: Remove the **summary-address** command in ISIS on PE.

Workaround 2: Change the BGP update source.

- CSCtn19178

Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf “A” and a new local label will not be reassigned.

Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf “B”, including:

- The vrf interface, for example, **no interface Gi1/0/1.430**.
- The same vrf process, for example, **no router ospf process id vrf vrf name**.

Run the following commands to verify whether you are facing this issue:

- **show ip bgp vpnv4 vrf A subnet** (this is for the working vrf)
- **show mpls forwarding-table labels local label**

Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

- **clear ip bgp mp-bgp neighbor soft in**
- **clear ip bgp mp-bgp neighbor soft out**

- CSCtn19496

Symptoms: Packet loss is seen when the service policy is applied on the tunnel interface. The **show hqf interface** command output shows drops in a particular queue with the following:

```
Scheduler_flags 177
```

The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.

Conditions: This symptom is observed when the service policy is applied on the tunnel/GRE interface, and when the source of the tunnel interface is the ATM interface(hwic-shdsl)

Workaround: There is no workaround.

Further Problem Description: The above-described symptom is seen only with the SHDSL link.

- CSCtn26785

Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

```
3845#sh int atm 1/0 stat
ATM1/0
      Switching path      Pkts In      Chars In      Pkts Out      Chars Out
      Processor           98170       10995040         1           68
      Route cache         0           0           98170       10995040
      Total               98170       10995040       98171       10995108
3845#

3845#sh cef int atm 1/0
ATM1/0 is up (if_number 5)
  Corresponding hwidb fast_if_number 5
  Corresponding hwidb firstsw->if_number 5
  Internet address is 64.65.248.174/30
  ICMP redirects are never sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Input features: Ingress-NetFlow
  Output features: Post-Ingress-NetFlow
  IP policy routing is disabled
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Hardware idb is ATM1/0
  Fast switching type 9, interface type 138
  IP CEF switching enabled
  IP CEF switching turbo vector
  IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 5(5)
  Slot Slot unit 0 VC -1
  IP MTU 4470
3845#
```

Conditions: The conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn32323

Symptoms: 802.1p information is not set on local generated traffic when bridge-dot1q is used on the DSL lines.

Conditions: Configure the device to transport 802.1p information over a DSL link connection, considering different CoS values for LAN and local generated traffic on the router.

```
interface ATM0.y point-to-point
  bridge-group <x>
  pvc 1/199
    bridge-dot1q encap <vlan>
    service-policy out <egress-policy>
```

Workaround: There is no workaround.

- CSCtn38996

Symptoms: All MVPN traffic is getting blackholed when a peer is reachable using a TE Tunnel, and an interface flap is done so that a secondary path can be selected. The multicast route does not contain a native path using the physical interface.

Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn39632

Symptoms: The RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

Conditions: This symptom occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than eight characters.

Workaround: Modify the keyring name to be less than eight characters.

- CSCtn48744

Symptoms: Memory leaks on OER border router while running the PfR-IPSLA configuration.

Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

Workaround: There is no workaround.

- CSCtn53094

Symptoms: The router crashes or generates the following error:

```
%SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process=
"Mwheel Process", ipl= 2, pid= 315
```

Conditions: This symptom is observed when toggling very fast between the **ip pim mode** and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

Workaround: Avoid fast toggling of the **pim mode** command if possible when it is only present on a single interface.

- CSCtn57655

Symptoms: A Cisco router running Cisco IOS Release 15.0M crashes during a SIP call.

Conditions: This symptom occurs when a Cisco router is running Cisco IOS Release 15.0M. This issue occurs only when the “callmonitor” CLI under “voice service voip” is configured.

Workaround: There is no workaround.

- CSCtn61834

Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.

Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keepalive message is received.

Workaround: There is no workaround.

- CSCtn63109

Symptoms: After reload or on a freshly upgraded router, Ping fails when the MTU is set above 1500 bytes on the FastEthernet 4 - WAN interface of a Cisco 800 series router connected directly to another router.

```
Router# ping 10.1.1.1 rep 5 df-bit size 1650
Type escape sequence to abort.
Sending 5, 1650-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with the DF bit set
.....
```

Conditions: This symptom is only observed with Cisco IOS Release 15.0(1)M4 and is specific only to Cisco 800 series routers. To be specific, only the Cisco 881SRST router is found faulty with the IOS, that is, c880voice-universalk9-mz.150-1.M4.bin so far. This issue is consistently seen with subinterface configurations based on the Fa4 interface.

Also, the following Traceback is noticed:

```
*Feb 28 15:26:19.639: %LINK-4-TOOBIG: Interface FastEthernet4, Output packet
size of 1664 bytes too big, -Traceback= 0x81056958z 0x81056EF8z 0x8112CBF4z
0x8200073Cz 0x82001264z 0x82001978z 0x820019D4z 0x8201BBF4z 0x8201C16Cz
0x8203F5C8z 0x8203FDACz 0x82D86B9Cz 0x81A1DC70z 0x819E6FD8z 0x819F6114z
0x8128C0CCz
```

Workaround: Remove and reconfigure MTU on the interface.

- CSCtn63325

Symptoms: The Cisco 1841 router crashes during firmware upgrade.

Conditions: This symptom occurs when microcode CLI is used during firmware upgrade on the Cisco 1841 router.

Workaround: There is no workaround.

- CSCtn68643

Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption.

```
ipv6 ospf encryption ipsec spi 500 esp null sha1
123412341234123412341234123412341234123412341234
```

or

```
ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
```

Workaround: There is no workaround.

- CSCtn70367

Symptoms: The IPSEC key engine crashes at sessions setup.

Conditions: This symptom is observed when setting up sessions with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. The crash happens on the IPSEC key engine. The crash occurs while UUT is establishing SAs that are requested. This issue is reproduced by clear crypto session on CES after all SAs are established.

Workaround: There is no workaround.

- CSCtn72853

Symptoms: Crash/watchdog timeout occurs at udb_classify_child.

Conditions: This symptom occurs due to various triggers like applying service-policy changes to complex level 2 or 3 policies where the same child/grand-child policy is used multiple times in the same parent.

Workaround: There is no workaround.

- CSCtn72939

Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.

Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.

Workaround: Configure bridge-group under that xconnect interface.

- CSCtn76183
Symptoms: A Cisco router configured for SIP NAT processing may crash.
Conditions: This symptom is observed while processing a SIP message from Cisco SPA phones (509, 524) in the inside network side.
Workaround: Use Cisco IOS Release 12.4(24)T3.
- CSCtn77211
Symptoms: Spurious memory access occurs at `cce_dp_ipc_cache_classify` at bootup.
Conditions: This symptom is observed when IPv6 SLA probes are configured, along with the firewall.
Workaround: There is no workaround.
- CSCtn87012
Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.
Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.
Workaround: Pick up the phone during the ringing OFF cycle.
- CSCtn90673
Symptoms: The Cisco 887 router crashes when sending baby jumbo frames downstream over the VDSL line.
Conditions: This symptom is observed when the VDSL interface, “interface e0”, is configured for Pppoe, a subinterface (that is, vlans), and an output service policy on interface e0. This issue is seen when an etherswitch interface is configured for trunking and baby jumbo frames or jumbo frames are sent downstream to the router. There is bidirectional traffic and the etherswitch vlan is then shut.
Workaround: Do not send baby jumbo frames or jumbo frames downstream to the Cisco 887 router. Do not shut the etherswitch vlan interface(s) when the router is routing traffic.
- CSCtn91807
Symptoms: A router acting as a voice gateway may crash due to a bus error.
Conditions: This symptom occurs when a button is pressed on a phone while using skinny. However, the exact conditions that cause this symptom are currently unknown.
Workaround: There is no workaround.
- CSCtn96521
Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.
Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.
Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.
- CSCtn97451
Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast peer** command on the router.
Conditions: This symptom occurs with the following conditions:
Router3 ---ebgp--- Router1 ---ibgp--- Router2

ROUTER1:

```

-----
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip pim sparse-mode
!

router ospf 100
  network 0.0.0.0 255.255.255.255 area 0
!

router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  neighbor 10.1.1.2 remote-as 1
  neighbor 10.1.1.3 remote-as 11 !

```

ROUTER2:

```

-----
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip pim sparse-mode
!
router ospf 100
  redistribute static
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

```

ROUTER3:

```

-----
interface Ethernet0/0
  ip address 10.1.1.3 255.255.255.0
  ip pim sparse-mode
!

router bgp 11
  bgp log-neighbor-changes
  network 0.0.0.0
  network 0.0.0.0 mask 255.255.255.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCto02448

Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

Conditions: This symptom is observed with the following conditions:

1. The neighbor is configured with soft-reconfiguration inbound.
2. The inbound routemap is not configured for the neighbor.
3. The non-routemap inbound policy (filter-list) allows the path.

Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto03446

Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

Conditions: This symptom occurs with a flat policy attached to a frame-relay interface with traffic shaping enabled.

Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto03506

Symptoms: The Gigabit Ethernet 0/2 interface on Cisco c3900 platforms is not seen by applications using snmp.

Conditions: This symptom occurs when Gigabit Ethernet 0/2 interface is not seen when you use the **snmpwalk** command.

Workaround: There is no workaround.

- CSCto07586

Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

Conditions: This symptom occurs with the following conditions:

1. Create a Cisco IOS image that does not have IPV6 enabled.
2. Enable BFD on an interface.
3. Configure an IPV4 static route with BFD routing through the above interface.

The IPV4 BFD session does not get established, so the static route does not get installed.

Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

- Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
- ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls>

- CSCto11025

Symptoms: When traffic streams are classified into multiple classes included with LLQ with qos-preclassify on the tunnel interface and the crypto map applied to an interface, packets are dropped on crypto engine on the Cisco 890 series router with buffers unavailable.

Conditions: This symptom is observed when IPSec and QoS are used when qos-preclassify is on the tunnel interface and a crypto map is on the main interface.

Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- CSCto13254

Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

```
Hash verification failed for file <temp location of profile>
```

Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

Workaround: Remove the profile from the Cisco IOS headend.

- CSCto14435

Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto23807

Symptoms: A Cisco device crashes when trying to transfer a call.

Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T2.

Workaround: There is no workaround.

- CSCto24338

Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0xFFFFFFFF
```

Conditions: This symptom occurs with NAT+SIP.

Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

- CSCto31265

Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

Workaround 1: Delete/readd the static route that generates Type7.

Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

Workaround 3: Execute **clear ipv6 ospf redistribution** command on ASBR.

- CSCto34196

Symptoms: When two Cisco 3945E routers are connected to each other and an IPSec VPN tunnel is established between them, any kind of traffic passing through the VPN tunnel takes about 10 milliseconds as Round Trip Time in case the Onboard Encryption Engine is used.

Conditions: This symptom occurs only when that traffic is encrypted by the Onboard Encryption Engine of Cisco 3945E (SPE250). After replacing the routers to Cisco 3945 (SPE150), the RTT is shorter than the one of Cisco 3945E.

Workaround: Use software encryption.

- CSCto42752

Symptoms: Removing the existing static policy and applying it back or adding the policy under that interface if it does not exist results in an error on standby.

Conditions: This symptom occurs when customers use high availability.

Workaround: Using the non-HA or standalone routine will fix the problem.

- CSCto45019

Symptoms: The router crashes when you remove the dialer interface and readd it and configure an IP address.

Conditions: This symptom occurs if you have continuous traffic passing through the router and going out of the dialer interface, and if you remove the dialer interface and readd it and then configure an IP address.

Workaround: Before configuring an IP address, configure encapsulation ppp or frame-relay but not hdlc.

- CSCto46716

Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto47524

Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder. A **show process memory sorted** command may initially show “MallocLite” growing. By disabling mallocite with the following, one may start to see the process “IP SLAs Responder” growing.:

```
config t
no memory lite
end
```

In at least one specific case, the leak rate was 80mb per day.

Conditions: This symptom is observed on a Cisco ASR 1002 router.

Workaround: Disable IP SLA on affected router, if possible.

- CSCto50255

Symptoms: Memory leak occurs while running the UDP echo operation.

Conditions: This symptom is observed when an UDP echo operation successfully runs. The leak is seen on every hundredth run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way to capture it is by monitoring and decoding the PC via the **show processes memory pid** command.

Workaround: There is no workaround.

- CSCto53332

Symptoms: A router configured for IPSEC accounting may display the following error message:

```
%AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
```

This does not seem to result in any impact apart from intermittently lost accounting messages.

Conditions: This symptom occurs when ipsec accounting is active.

Workaround: There is no workaround.

- CSCto55708

Symptoms: There is a build error due to a missing ‘ ’ in a printf statement, only in dsgs, due to compiler-specific issues.

Conditions: This symptom occurs due to a missing ‘ ’ in a printf statement only in dsgs due to compiler-specific issues.

Workaround: There is no workaround.

- CSCto63417

Symptoms: A spurious access or crash occurs after applying the service policy.

Conditions: This symptom occurs specifically when applying service-policy type access-control. This issue occurs when a large amount of traffic is being sent to the interface. The class-map uses RegEx in the match statement.

For example:

```
class-map type access-control match-any bittorrent
  match start l2-start offset 54 size 32 regex "GETinfo_hash="
  match start l2-start offset 54 size 32 regex
"[a|A][z|Z][v|V][e|E][r|R]
```

Workaround: Apply the service policy during low traffic or do not use RegEx in match statements.

- CSCto63954

Symptoms: A router with GETVPN configurations is continuously crashing.

Conditions: This symptom is seen with GETVPN-related configurations with the fail-close feature activated.

Workaround: There is no workaround.

- CSCto68554

The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

These vulnerabilities are:

- Memory leak in Cisco IOS Software
- Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are not available.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw>.

- CSCto69071

Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.

Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.

Workaround: There is no workaround.

- CSCto71744

Symptoms: FXO interfaces with the cable-detect feature enabled will automatically transition to the off-hook state when no PSTN battery voltage is detected, and remain off-hook for a duration of up to 1 minute. This condition violates regulatory telecom standards in several countries, including but not limited to the USA and Canada.

The failing clauses of regulatory standards are as follows:

- TIA-968-B 5.1.11.3
- TIA-968-B 5.1.12.3
- Industry Canada CS-03 Part I, Issue 9 December 2010

Conditions: This symptom occurs when the FXO interface is up, and the cable is connected to PSTN. Any interruption of the PSTN battery to FXO induces the off-hook condition, and the port does not transition back to on-hook for up to 1 minute.

Workaround: Disable the cable-detect feature in the FXO <config-voiceport> prompt. You can enable the feature in topologies that are not subject to regulatory standards (that is, on-premise installations).

- CSCto75350

Symptoms: A crash occurs at udb_classify.

Conditions: This symptom occurs when level 3 HQoS is configured. The second-level policy from under class-default is removed. This is followed by traffic, either self-generated through IP SLA or possibly through data traffic traversing.

Workaround: There is no workaround.

- CSCto81814

Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

Conditions: This symptom is only observed when ECDSA certificates are used for IKEv2, and not with RSA certificates or with IKEv1.

Workaround: There is no workaround.

- CSCto86833

Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DN's with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

Workaround: If possible, reduce the number of voice ports automatically generated by the number DNs and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- CSCto88686

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip>

- CSCtq25682

Symptoms: The router crashes after configuring “gw-accounting file”.

Conditions: This symptom occurs if the router’s memory usage is already over 80 percent utilization, and after configuring “gw-accounting file”, the following log message is displayed:

```
%VOICE_FILE_ACCT-4-MEM_USAGE_HI_WATERMARK: System memory on high usage
(81/100). Stopping processing new event log for now.
```

After this log, when the cdrflush-timer expires, the router crashes.

Workaround: Do not enable “gw-accounting file” when the router’s memory utilization is already over 80 percent.

- CSCtq35297

Symptoms: Cisco c880 images do not get compiled.

Conditions: This symptom occurs during compilation of Cisco c880 images.

Workaround: There is no workaround.

- CSCtj29382

Symptoms: When cellular interface passes packets and users configure “tx-ring-limit” on cellular interface, the system crashes.

Conditions: This symptom occurs under the following conditions:

1. Traffic runs through cellular interface.
2. Change “tx-ring-limit” on cellular interface with traffic running in the background.

Workaround: Stop the traffic and change “tx-ring-limit”.

- CSCtn19027

Symptoms: The **show mediatrace responder sessions brief** command crashes the router.

Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.

Workaround: There is no workaround. Avoid issuing this impacted **show** command.

- CSCto77537

Symptoms: Calls between SME-CUBE fail due to no audio path when the originating leg is G729r8 and the CUBE preferred codec list contains g729br8.

Conditions: This symptom occurs under the following conditions:

- CUBE ISR: c3845-ipvoicek9-mz.151-4.M
- There is no audio path after call setup. The call either disconnects (case SIP-H323) or stays up without voice path (case SIP-SIP).

The call flow is as follows:

```
OriginatingCluster--> SAF SIP Trunk ---> SME ---> CUSP --> CUBE (originating)
--> CUSP <----->
CUSP --> CUBE (Terminating) --> CUSP --> SME --> SAF H323 Trunk --->
TerminatingCluster
```

```
CUBE codec Config:
voice class codec 1
codec preference 1 g729r8
codec preference 2 g729br8
codec preference 3 g711ulaw
codec preference 4 g722-64
```

Workaround 1: Remove the g729br8 codec in the voice-class codec config on CUBE to ensure that CUBE will offer only g729r8 in the outgoing offer.

Workaround 2: Change the Originating SME, SIP trunk to Originating CUBE from DelayOffer to EarlyOffer.

Workaround 3: Configure a transcoder.

- CSCtq64951

Symptoms: The following message is displayed:

```
%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto
functionality with securityk9 technology package license.
```

The **show platform cerm** command output shows all tunnels in use by SSLVPN.

```
Number of tunnels      225
...
SSLVPN   D      D      225   N/A
```

The **show webvpn session context all** command output shows no or very few active sessions.

```
WebVPN context name: SSL_Context
```

```
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
```

Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq36726

Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual-access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

Workaround: Reconfigure the Virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

- CSCtn76183

The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat>

Open Caveats—Cisco IOS Release 15.1(4)M

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(4)

m. All the caveats listed in this section are open in Cisco IOS Release 15.1(4)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtr44373

Symptoms: This is a platform independent issue. Users cannot receive a call through a BRI port. A fast tone will be heard.

Conditions: This symptom is observed on a newly released image.

Workaround: Configure forward digital all in the CLI.

The following example shows a sample configuration:

```
dial-peer voice 111 pots
```

```
destination-pattern 111
```

```
!direct-inward-dial
```

```
port 2/0
```

```
forward-digits all
```

Resolved Caveats—Cisco IOS Release 15.1(4)M

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(4)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsm23548

Symptoms: The standby supervisor may crash when pasting in a crypto certificate on the active supervisor.

Conditions: This symptom is observed in configuration mode when applying a certificate.

Workaround: There is no workaround.

- CSCsr17680

Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

Conditions: This symptom is observed when sending a request to a particular server on a server-group.

Workaround: There is no workaround.

- CSCsv30540

Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and a traceback are seen.

Conditions: These symptoms are observed when the **show running-config/write memory** command is issued.

Workaround: There is no workaround.

- CSCsx62864

Symptoms: Active RP may reload due to IOSD failure if clear crypto session is done after attaching the gdoi crypto map.

Conditions: This symptom is observed when the following actions are taken:

3. remove the gdoi crypto map from the interface connected to the Key Server (KS)
4. clear crypto sessions
5. attach the crypto map again

Now, if the crypto sessions are cleared, IOSD will restart and will result in an RP reload.

Workaround: Avoid clearing crypto sessions after attaching a crypto map. Wait for the GM to send the registration in default manner and allow the KS to send the SAs.

- CSCsx65975

Symptom: The router may reset unexpectedly during an ISSU process from RLS2 to RLS3.

Conditions: This symptom is observed when all of the following conditions exist:

1. SSH rsa keys are configured
2. the RLS2 image does not have CSCsx65975 integrated
3. the RLS3 image does not have CSCsz05125 integrated

This symptom will not occur if the SSE keys are zeroized (removed). It will not occur if RLS2 has CSCsx65975 integrated; nor will it occur if RLS3 has CSCsz05125 integrated.

Workaround: The workaround is only required if all three conditions above exist. Zeroize your SSE rsa keys before the ISSU process:

```
asrlk(config)#crypto key zeroize rsa
```

Then, after the ISSU process, create new keys:

```
asrlk(config)#crypto key generate rsa
```

Further Problem Description: Enter the **show ip ssh** command to determine whether SSE is enabled or disabled. (you cannot tell by entering the **show running configuration** command).

- CSCsy54233

Symptoms: "Exception_reserve_memory" is invalid in a UNIX image.

Conditions: This symptom is observed in a UNIX image, which do not support "exception_reserve_memory."

Workaround: There is no workaround.

- CSCsz18634

Symptoms: An input/output rate is always displayed with "0" in interface status, even though packets are flowing on the ports normally.

```
show int gig 4/1 output GigabitEthernet4/1 is up, line protocol is up (connected)
.....
Output queue: 0/40 (size/max) 30 second input rate 0 bits/sec, 0 packets/sec
```

```
<<<<<<<<<< 30 second output rate 0 bits/sec, 0 packets/sec <<<<<<<<<< 3411001
packets input, 567007874 bytes, 0 no buffer Received 818876 broadcasts (725328
multicasts)
```

Conditions: This symptom is observed on a Cisco 3750 that is running Cisco IOS Release 12.2(46)SE, as well as a Cisco 4500 and Cisco 4900M that are running Cisco IOS Release 12.2(46)SG and Cisco IOS Release 12.2(53)SG1.

Workaround: This issue is a cosmetic issue and does not affect the functionality of the switch or the traffic flow.

Use the value of the **show int gigx/y count detail** command to see the raw statistics.

The rate shown in the **sh int** command uses a complex convergence algorithm. If the rate changes from X to Y, it could take several minutes (15-30) for the rate to converge from X to Y. The rate must be steady and should be sent from a tester to confirm that the convergence is happening correctly.

Or, execute reload.

Further Problem Description: On the Cisco 3570 platform, the fix is in Cisco IOS Release 12.2(53)SE. On the Cisco 4500/4900M, the fix for this bug is scheduled to be in Cisco IOS Release 12.2(53)SG2 and Cisco IOS Release 12.2 (50)SG7.

- CSCsz29564

Symptoms: ASR starts using the new SA as soon as it received. This causes traffic loss in the network.

Conditions: This symptom is observed if a GM misses the rekey. Communication to this GM from the ASR fails because the ASR immediately begins using the new SA to encrypt, rather than waiting for the GM that missed the rekey to reregister.

Workaround: There is no workaround.

- CSCsz35913

Symptoms: An interface goes down in spite of carrier-delay configuration.

Conditions: This symptom is observed on a PA-E3, when the serial interface carrier-delay is configured for one second and any of the alarms (AIS, LOF) are generated for less than or equal to one second.

Workaround: Increase the carrier-delay.

- CSCsz44301

Symptoms: NHRP is not registered to the root hub.

Conditions: This symptom is observed after an RP switchover.

Workaround: There is no workaround.

Further Problem Description: During platform RP switchover, the root hub is not seeing NHRP registration messages from first-level hubs.

- CSCsz92328

Symptom: None of the interfaces come up after SSO is done with configuration with self-signed certificates.

Conditions: This symptom is observed under the following conditions:

1. RSA self-signed certificate is generated on the router
2. Router is reloaded
3. SSO is done on the router

Workaround: After reload, remove and add the self-signed certificate.

- CSCta02570
Symptoms: The IOSd resets when 1500 dVTIs are brought up at the same time.
Conditions: This symptom is observed when a large number of dVTIs are brought up at the same time.
Workaround: There is no workaround.
- CSCta14505
Symptoms: No source group (SG) entry forms in the network for PIM sparse-mode groups. This leads to traffic failures.
Conditions: This symptom is observed when PIM-SM is configured in the network and traffic is sent for PIM-SM groups.
Workaround: Shut down the upstream interface, remove the IP address, configure it again, then perform a **no shutdown** on the interface.
- CSCta22480
Symptom: Memory leaks are not removed after reload on a Cisco ASR.
Conditions: This symptom is observed after the following sequence of events:
 1. After making some stress calls, the **show mem deb leak summ** command is entered in order to see the memory leaks.
 - 2) The router is reloaded to remove the leaks.
 - 3) Once the router is up, the **show mem deb leak summ** command is entered again to check for leaks.
 Result: None of the memory leaks are removed.
Workaround: There is no workaround.
Further Problem Description: The **show mem deb leak summ** command is a debug command that is not used under normal router operations and that therefore does not affect normal router behavior.
- CSCta22746
Symptoms: A Cisco ASR1000 may crash when a large number of DMVPN tunnels have been brought up and a user enters the **sh cry isakmp sa** command.
Conditions: This symptom is observed on a Cisco ASR1K with RP2, configured as IPsec DMVPN Phase3 spoke, and when multiple routing protocols are configured for overlay routing.
Workaround: There is no workaround.
- CSCta26520
Symptoms: The following traceback is seen:

```
%IDBINDEX_SYNC-3-IDBINDEX_LINK: Driver for IDB type 0 changed the Identity of
interface "Tunnell" without deleting the old Identity first
```

 Conditions: This symptom is observed when numerous tunnel interfaces are rapidly added and removed.
Workaround: There is no workaround
- CSCtb20400
Symptoms: A Cisco ASR may crash.

Conditions: This symptom is observed when certain IPv6 crypto configurations are unconfigured when configurations are copied from tftp to the running config. The problem is not seen when an actual CLI is used (as opposed to the **copy tftp running** command) on the router to unconfigure IPv6 IPsec. The problem also seems specific to RP2 since only the RP2 router has crashed so far. It does not seem to affect RP1.

- Workaround: Use CLI to unconfigure instead of configuring via the **copy tftp running** command.
- CSCtb42862

Symptoms: A Cisco 3845 router crashes due to illegal memory access.

Conditions: The symptom is observed in a scale testing environment which has eight key servers and 20 GM routers (simulating 2000 group members) and when there is unicast rekeying. The GM router crashes in steady state (no traffic). This seems to be intermittent.

Workaround: There is no workaround.

- CSCtb74547

Symptom: A Cisco ASR 1000 Series Aggregation Services router DMVPN HUB reloads at process IPSEC key engine.

Conditions: This symptom is observed when the dual DMVPN with shared tunnel protection feature is enabled.

Workaround: There is no workaround.

- CSCtc00851

Symptoms: The output of the **show mfib table** command on a line card can show tables not in “sync” state, and instead in “disconnecting” or “connecting” state for some time (minutes). In this state the multicast forwarding tables are not being updated and may be out of sync with the active RP.

Conditions: This symptom is observed on line cards or the redundant RP on a distributed router. It is usually associated with conditions of high CPU due to large numbers of routing updates in a scaled configuration.

Workaround: The **clear mfib table** command may clear the problem. Alternatively, the affected line cards may need to be reloaded.

Further Problem Description: Often the problem will be accompanied with error messages relating to MFIB connectivity to the multicast routing information base.

- CSCtc67457

Symptom: A Cisco ASR 1000 Series RP2 crash occurs with the process IKMP.

Conditions: This symptom is observed with GetVPN Group Member Configs with vrf-lite.

Workaround: There is no workaround.

- CSCtd59027

Symptoms: The device crashes due to a bus error.

Conditions: This symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCtd92821

Symptoms: A router continuously crashes upon bootup.

Conditions: The symptom occurs if SSH is configured and if the router is in SSO mode.

Workaround: Remove SSH keys or use NONE mode for RPR.

- CSCte39643
Symptoms: If PfR receives an EIGRP route change, the router may unexpectedly reload.
Conditions: This symptom is observed with PfR and EIGRP configurations. It is observed some time after PfR receives an EIGRP route change, but before the previous EIGRP route is removed in the routing table, when PfR tries to recycle a previous EIGRP route.
Workaround: There is no workaround.
- CSCte58962
Symptoms: If an OSPF instance is being redistributed by some other routing protocol but is never activated by configuring “router ospf x”, the standby RP can crash during a subsequent execution of the **no router ospf x** command.
Conditions: The symptom is observed on systems with redundant RPs and only if the standby is reloaded after the redistribution is removed.
Workaround: Have “router ospf x” configuration lines for all the OSPF instances being redistributed by other protocols.
- CSCte83779
Symptoms: A Cisco ASR 1000 Series Aggregation Services router may crash.
Conditions: The symptom is observed when DMVPN is configured with GETVPN. It is only seen when running a specific script for ASRs.
Workaround: There is no workaround.
- CSCte91471
Symptoms: Clock synchronization with the NTP server could be lost for several hours if router (NTP client) runs NTPv4.
Conditions: The symptom is observed if the router clock is reset (for example: by using the **clock set exec** command). The router then takes a long time to synchronize again.
Workaround: There is no workaround. The clock will automatically synchronize after few hours.
- CSCte92659
Symptoms: The router loses some memory due to flow id.
Conditions: The symptom is observed with a 32k session scaling scenario and with the PPP session flapping when accounting associated with flow id is configured.
Workaround: There is no workaround.
- CSCte94221
Symptoms: A PPP connection over CDMA link is flapping.
Conditions: This symptom is observed when using Cisco IOS Release 15.0M.
Workaround: Shut / no shut the interface and wait for 2 minutes.
- CSCte98852
Symptoms: When the broadband accounting accuracy feature (for example, “subscriber accounting accuracy”) is configured and “service accounting” is enabled, a duplicate session accounting start (with unique session ID) message is sent out, creating two entries in the AAA server.
Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router. The issue is observed only when the accounting accuracy feature and service accounting are enabled.

Workaround: There is no workaround as the accounting accuracy may be off as much as 10-seconds worth of byte-counts if the feature is turned off. You could configure the following:

1. **aaa accounting delay-start**
2. **aaa accounting include auth-profile [delegated-ipv6-prefix, framed-ip-address, framed-ipv6-prefix].**

- CSCtf23298

Symptoms: High CPU usage occurs.

Conditions: This symptom occurs when a Terminal Access Controller Access-Control System (TACACS) server is configured with a single connection.

Workaround: Remove single connection option.

- CSCtf36117

Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

Workaround: There is no workaround.

- CSCtf53537

Symptoms: Serial interfaces are messed up in second redundancy switchover.

Conditions: This symptom is observed upon second switchover in sb_throttles.

Workaround: The issue is due to a change in if_numbers of serial interfaces.

- CSCtf54561

Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf vrf-name** command is issued.

Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

Workaround: The command should not be entered when many topology changes occur on interface flaps.

- CSCtf56107

Symptoms: A router processing an unknown notify message may run into a loop without relinquishing control, kicking off the watchdog timer and resulting in a software-based reload.

Conditions: The symptom is observed when an unknown notify message is received.

Workaround: There is no workaround.

- CSCtf72328

Symptoms: BFD IPv4 Static does not fully support AdminDown.

Conditions: The symptom is observed with the following setup and configuration:

```
Router 1: interface e0/0 ip address 192.168.1.1 255.255.255.0 bfd interval 51 min_rx
51 multiplier 4 bfd echo no shut exit
interface loopback 0 ip address 10.10.1.1 255.255.0.0 exit ip route static bfd e0/0
192.168.1.2 ip route 10.20.0.0 255.255.0.0 e0/0 192.168.1.2
Router 2: interface e0/0 ip address 192.168.1.2 255.255.255.0 bfd interval 51 min_rx
51 multiplier 4 bfd echo no shut exit
interface loopback 0 ip address 10.20.1.1 255.255.0.0 exit
```

```
ip route static bfd e0/0 192.168.1.1 ip route 10.10.0.0 255.255.0.0 e0/0 192.168.1.1
interface e0/0 no ip route static bfd e0/0 192.168.1.1
```

Though the BFD state is **DOWN**, the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtf87039

Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

Workaround: There is no workaround.

- CSCtf89408

Symptoms: A crash may be seen on switchover while the session replays on the standby.

Conditions: The symptom is observed if the nas-port-id in service profile is null.

Workaround: There is no workaround.

- CSCtg01020

Symptoms: Due to an invalid SPI (value 0), phase 2 is not established between two Cisco ASR 1000 series routers when a VPN tunnel is configured.

The output of “show crypto ace spi” shows “Normal SPI allocated 61140” or in a show tech look for “SPI allocated.....61440” on one of the routers.

The peer might issue an error about an invalid SPI with value zero.

Conditions: The symptom is observed when the ASR router has been up for weeks. The failure will show up once we've run out of SPIs to allocate on the hardware.

Workaround: The tunnel will come up after a reload of the ASR as all the allocated SPIs will be freed. SPIs will be leaked only when a phase 2 negotiation fails. SAs that expire due to hitting their lifetime will not leak their SPIs. Therefore, if the network is stable and all tunnels are properly configured and all endpoints remain reachable and no negotiations fail, the impact of this defect can be minimized.

- CSCtg13269

Symptoms: On peers of Route Reflectors (RR), the received prefixes counter shows an incorrect number when session flaps occur during a network churn.

Conditions: The symptom is observed with BGP RRs.

Workaround: Use the **clear ip bgp *** command.

- CSCtg22674

Symptoms: The router experiences high CPU for several minutes due to a “MPLS TE LM” process.

Conditions: This symptom occurs when a router has many (perhaps as few as 100) MPLS TE tunnels that traverse over a link that experiences repeated flapping in a short duration.

Workaround: There is no workaround.

Further Problem Description: Use the command **show process cpu** to determine CPU utilization. If this problem exists, the MPLS TE LM process holds greater than 90% resources for 5 minutes or more.

```
CPU utilization for five seconds: 100%/0%; one minute: 100%; five minutes: 100% PID
Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 216 867694836 18357673 47266
99.67% 99.09% 99.11% 0 MPLS TE LM
```

- CSCtg41606

Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multi-access interface (for example, ethernet) then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

Conditions: The symptom could occur when the upstream device does not support proxy arping.

Workaround: Use the **reverse-route remote-peer <next-hop-ip>** command instead of just **reverse-route**.

- CSCtg44097

Symptoms: The connect-Info(77) attribute is sent twice in a Pre-Auth Access-Request, when it should only be sent once.

Conditions: The symptom is observed when the outbound service policy and LLID authorization feature are configured.

Workaround: There is no workaround.

- CSCtg58786

Symptoms: When an external interface on the BR is shut down, the BR could crash.

Conditions: This symptom is observed if more than 1000 Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down.

Workaround: There is no workaround.

- CSCtg60228

Symptoms: In a rare condition of using the **config replace <>** command to remove all the bgp configurations that contain bgp peers as part of a peer-group, the router may crash due to a timing issue between the bgp tasks.

Conditions: This symptom is observed when “config replace <>” is used to replace old router configs when bgp has lots of peers as part of the peer-group, and when the configs are replaced with new config that do not have bgp configurations.

Workaround: Do not use the **replace config <>** command.

- CSCtg64175

Symptoms: The ISIS route is missing the P2P link. It is mistakenly marked as “parallel p2p adjacency suppressed.”

Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCtg67346

Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show “Di1 DDR: dialer_fsm_pending() di1.”

Conditions: The conditions are unknown at this time.

Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCtg68047

Symptoms: The router reloads.

Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

Workaround: Wait until the tunnels are shut down before issuing the **show** command.

- CSCtg72481

Symptoms: Spurious memory access is seen with QoS configurations.

Conditions: The symptom is observed only when sending the traffic for a while.

Workaround: There is no workaround.

- CSCtg73631

Symptoms: Spurious access or crash.

Conditions: EIGRP undergoes a route delete event for a route that is both redistributed and learned as an external. The redistributed route is deleted and the external route promoted. An error in the route deletion codepath may result in spurious access or crash.

Workaround: There is no workaround.

Further Problem Description: The symptom is not present in Cisco IOS Release 15.0(1) M4.

- CSCtg75452

Symptoms: RP crashes in dual RP system after doing a **config replace** on POS-configured SDH link.

Conditions: The symptom is observed if you configure a POS SDH link on a 1XCHSTMOC12/DS0 SPA port and do a **config replace** to a basic router configuration that includes redundancy mode change. This crashes the RP and produces a core file.

Workaround: There is no workaround.

- CSCtg75627

Symptoms: The **clear ip route vrf <vrf-name> <address>** command removes the route to the destination network if the host address (rather than the network address) is used.

Conditions: The symptom is observed when the **clear ip route vrf <vrf-name> <address>** command is entered. Other conditions are not known at this time.

Workaround: **Shut** then **no shut** the interface.

- CSCtg84969

Symptoms: The output of **show ip mfib vrf <vrf name> verbose** may show the following line, and multicast traffic may not be hardware switched:

```
"Platform Flags: NP_RETRY RECOVERY HW_ERR"
```

Conditions: The symptom is observed on a dual RP Cisco 7600 series router with linecards after multiple reloads or SSO switchovers. When the symptom occurs the output of **show ip mfib vrf <vrf name> verbose** on the standby SP will show some lines preceded with "###" where an interface name is expected.

Workaround: There is no workaround.

- CSCtg89555

Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

Conditions: This symptom is observed when configuring an IP address after multicast has been configured on a dot1Q interface.

Workaround: Perform a **shut/no shut** of the interface.

- CSCtg91572

Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

Workaround: There is no workaround.

- CSCtg93243

Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used, packets get forwarded after decryption as expected.)

Workaround: There is no workaround.

- CSCtg96280

Symptoms: Cisco VSA “prefix” is not working.

Conditions: The symptom is observed when Cisco VSA “prefix” is used.

Workaround: There is no workaround.

Further Problem Description: The issue follows from the fix for CSCte35678.

- CSCth01526

Symptoms: The MDT interface is deactivated and activated after an SSO.

Conditions: After an SSO switchover, the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

Workaround: There is no workaround.

- CSCth05533

Symptoms: A memory leak occurs in the IPSec key engine.

Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation services router. It is seen with a VPN hub that has more than 500 spokes.

Workaround: There is no workaround.

- CSCth09200

Symptoms: The **show bgp all peer-group <group name> summary** or **show ip bgp all peer-group <group name> summary** CLI commands do not show peer-group summary information for all the address families.

For Cisco IOS 12.2(31)SG and 12.2(31)SGA releases, these CLI commands may crash the router.

Conditions: This symptom is observed if:

1. There is a description for the peer-group
2. There is a description for the first neighbor member of the peer-group.

The above two conditions can be determined in the show running-config.

3. The first entry in attribute hash table is non empty (internal)

Workaround: Use the **sh ip bgp <address-family> [<safi>] peer-group <group name> summary** command instead.

- CSCth15105

Symptoms: BFD sessions flap after unplanned SSO (test crash).

Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

Workaround: There is no workaround.

- CSCth16962

Symptoms: The primary KS KEK timer gets stuck or reset to zero after a GDOI policy change and rekey. Once the KEK timer gets stuck/reset to zero, there are repeated rekeys, which will impact the whole GET VPN domain. The trigger occurs after a failure event in the primary key server and the secondary key server becomes primary followed by a policy change.

Conditions: This symptom occurs when the KEK timer gets stuck at zero and there are repeated rekeys to GMs, resulting in a rekey storm.

Workaround: There is no workaround.

- CSCth18616

Symptoms: Decode of Framed-IPv6-Prefix fails.

Conditions: The symptom is observed whenever Framed-IPv6-Prefix is included in a RADIUS profile.

Workaround: There is no workaround.

- CSCth19516

Symptoms: A router crashes if PFR and SAF are enabled on the same device.

Conditions: The symptom is observed when SAF is enabled and PFR has multiple links. When the network gets congested or delay is seen and if there is a changeover from IN-POLICY state to OOP, the router crashes.

Workaround: Disable SAF completely and reload the router.

- CSCth20862

Symptoms: A router crashes upon changing the “ipsec gre tunnel” configuration. The crash is seen when the “invalid SPI” message is displayed. This message is normal in IPSec settings, but is more often seen in a session flap situation.

Conditions: The symptom is observed when two IPSec GRE tunnels are configured on a PE router. The crash is seen after changing the tunnel’s destination and flapping the tunnel. At certain times the issue is seen when just flapping the GRE tunnel.

Workaround: There is no workaround.

- CSCth23354

Symptoms: Packets are not reaching the proper queue.

Conditions: The symptom is observed when class-map is configured with VLAN.

Workaround: There is no workaround.

- CSCth29393

Symptoms: Downstream traffic (to the subscriber) is not forwarded. Only upstream counters are increasing.

Conditions: The symptom is observed with the **show sss session detail** command with PXF output.

Workaround: Clear the affected SSS session.

- CSCth37580

Symptoms: Dampening route is present even after removing “bgp dampening.”

Conditions: The symptom is observed under the following conditions:

- DUT connects to RTRA with eBGP + VPNv4
- eBGP + VPNv4 peer session is established and DUT
- DUT has VRF (same RD) as route advertised by RTRA

In this scenario, when DUT learns the route, it will do the same RD import and the net topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

Workaround: There is no workaround.

- CSCth38303

Symptoms: A Cisco router running Cisco IOS with an ISG feature set can crash at radius_remove_pkt_id.

Conditions: This symptom is observed when radius-proxy is configured and the AZR reboot feature comes into play with immediate retransmits of accounting ON/OFF messages.

Workaround: If the downstream device works correctly without sending retransmits immediately after sending the first packet, the ISG should not crash.

Alternate Workaround: Do not configure the forward method list under radius-proxy. With this workaround, radius-proxy responds to the accounting message immediately and there will be little chance of getting a retransmit from the downstream client.

- CSCth40213

Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

Workaround: There is no workaround.

- CSCth42798

Symptoms: Memory can be corrupted.

Conditions: This symptom is observed when BGP is in read-only mode and attributes are deleted before the networks.

Workaround: There is no workaround.

- CSCth46156

Symptoms: Sometime the ISIS nexthop is not generated because the MT ISIS neighbor is missing in LSP.

Conditions: In MTR support case, enabling ISIS on multicast topologies after ISIS adjacency is established on IPv4 unicast base topology.

Workaround: “Shut” then “no shut” the interface.

- CSCth47686

Symptoms: A crash is seen on the EXEC process on a GM.

Conditions: This symptom is observed when the same GDOI map is applied to multiple interfaces and the **sh crypto gdoi gm replay** command is entered.

Workaround: There is no workaround.

- CSCth64316

Symptoms: Unable to configure “radius-server” using SNMP set.

Conditions: The symptom is observed when you configure via SNMP MIB.

Workaround: Radius server can be configured through the CLI.

- CSCth66604

Symptoms: ISSU incompatibility due to different versions of a protocol (NTP v3 and NTP v4).

Conditions: The symptom is observed with an ISSU upgrade or downgrade.

Workaround: Unconfigure the CLIs causing MCL errors and repeat the ISSU process again.

- CSCth66813

Symptoms: Traffic flows only on one side while sending bi-directional traffic.

Conditions: This symptom is observed after disabling or enabling “atm route-bridged ip.”

Workaround: “Shut” then “no shut” the interface.

- CSCth73173

Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCth85294

Symptoms: A PIM neighborhood is not established with the remote PE and RP for the MVRFs.

Conditions: This symptom is observed with traffic, after removal and restoration of mvrfs. Traffic does not flow properly since the PIM neighborhood is not established with the remote PE and RP for those MVRFs.

Workaround: There is no workaround.

- CSCth85618

Symptoms: Extra syslog gets printed but no other functionality is impacted.

Conditions: This symptom occurs under normal conditions.

Workaround: There is no workaround.

- CSCth90147

Symptoms: Router will respond to an RS with an RA.

Conditions: The symptom is observed when you configure the command **ipv6 nd ra suppress**. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

Workaround: Use an ACL to block the reception of RS packets.

- CSCth91984

Symptoms: Standby resets continuously.

Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

Workaround: Unconfigure the **set extcommunity** command.

- CSCth93218

Symptoms: The error message "%OER_BR-4-WARNING: No sequence available" displays on PfR BR.

Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

Workaround: There is no workaround.

- CSCti01036

Symptoms: A Cisco ASR1000 series router crashes on the Radius Process.

Conditions: This symptom is observed on a Cisco ASR 1000 series router with Radius AAA services enabled. When the Radius server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.

Workaround: Prevent the AAA server from sending empty VSA strings.

- CSCti02076

Symptoms: On a system running Cisco IOS, after unconfiguring an IPv6 link-local address from an interface, any global ipv6 addresses may disappear.

Conditions: This issue may occur on systems running Cisco IOS when IPv6 is being configured. This issue occurs if an attempt is made to remove the IPv6 link-local address without use of the *link-local* keyword.

Workaround: There is no workaround.

- CSCti03199

Symptoms: During switchover, standby crashes after every recovery due to config-sync.

Conditions: The symptom is observed when the standby tries to sync with the active and when "crypto pki trustpoint" is configured with an unavailable port-channel as source-interface.

Workaround: There is no workaround.

- CSCti03808

Symptoms: A Cisco 7200 may crash with a fatal error.

Conditions: This symptom is observed only when PA-POS-1OC3 and C7200-VSA port adapters are installed and the encrypted traffic is being sent through the POS interface. The problem is more likely as traffic load increases.

Workaround: Use a different POS port adapter or VAM module instead of the VSA encryption module.

Further problem description: During investigation the router would also occasionally hang instead of crash. With the fix for this symptom the hangs were not seen.

- CSCti13286

Symptoms: Putting this configuration on a router:

```
router rip version 2 no validate-update-source network 10.0.0.0 no auto-summary!
address-family ipv4 vrf test no validate-update-source network 172.16.0.0 no
auto-summary version 2 exit-address-family
```

and doing a reload causes the "no validate-update-source" statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti17841

Symptoms: Removing “match condition” from a class map crashes the router.

Conditions: The symptom is observed when you remove “match condition” from a class map.

Workaround: There is no workaround.

- CSCti18615

Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP out-of-sync with the active RP. A and F flags are missing from the multicast forwarding base entries.

Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, the router is in HA mode SSO, and is reloaded from the RP.

Workaround: Perform a Shut/no shut of the affected interfaces.

- CSCti20016

Symptoms: Two issues occur:

1. When “no bgp default ipv4-unicast” is configured, the dynamic neighbors do not get established
2. If peer-groups have multiple sessions configured, then even if the neighbor belongs to the peer-group, it does not send this capability.

Conditions: These symptoms occur when multiple sessions are configured.

Workaround: For the first issue, if the dynamic neighbor peer-group is activated for other topologies, configure a single session. Configuring a single session also resolves the second issue.

Further Problem Description:

1. For the first issue, when **default ipv4-unicast** was disabled in the peer-group member parse function, we do not create a neighbor topology for the IPv4 topology at all. Hence, the dynamic neighbors never come up, resetting due to notification that afi/safi is not supported. For normal neighbors, activation needs to be done for each address family. So neighbor topologies are created at configuration time. But for dynamic neighbors, although the peer-group is explicitly configured for each address family, the actual neighbor creation occurs when we get an “open” from the neighbor address, within the dynamic neighbor range configured wherein the pgrp member parse function is called with afi as router mode. But policy commands are not accepted if **default ipv4-unicast** is disabled in router mode, and similarly neighbor topos cannot be created in such a case. So, when the new dynamic neighbors trying to be created in such a scenario are rejected, the symptom occurs. An exception has to be made for dynamic neighbors.
 2. The second issue is applicable for all peer-group members, not just dynamic neighbors. The `bgp_neighbor_send_multisession_cap_allowed()` returns “true” only if the multisession capability is configured on the neighbor. If the multisession is configured on the peer-group, and then members do not inherit this property, even though the member accepts the multisession neighbor capability, when the neighbor sends the capability, a single session cap is sent. The peer router keeps rejecting with unsupported capability notification and hence the neighbor never comes up. So peer-group flags should also be considered when any member is checked in `cap_allowed` function.
- CSCti22091
- Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

Conditions: The symptom is observed when PfR is configured with the following conditions:

1. list > application > filter > prefix-list
2. Learn > traffic-class: keys
3. Learn > traffic-class: filter > ACL

Workaround: There is no workaround.

- CSCti22544

Symptom: IKE fails to come up while using RSA signature. PKI debugs show the following message:

```
PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
```

Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example,

```
crypto pki trustpoint yni-u10 enrollment url http://yni-u10:80 vrf coke
```

Workaround: There is no workaround.

- CSCti25319

Symptoms: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute Open Shortest Path First (OSPF) is configured.

Conditions: This symptom occurs only for those configurations in which a network mask covers multiple supernets. For example, for the following network statement, router ospf 1 network 192.168.0.0 0.255.255.255 area 0 the above mentioned symptom occurs if the interfaces are configured with IP addresses as follows: ip address 192.168.0.1 255.255.255.0 ip address 192.168.1.1 255.255.255.0 and so on.

Workaround: Enable OSPF using the interface command “ip ospf <AS> area.”

Alternate Workaround: Configure multiple network statements with mask/wildcard equal to supernet as shown in the example below:

```
router ospf 1 network 192.168.0.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255 area
0
and so on.
```

- CSCti28710

Symptoms: Chunk memory leak is observed on oer_mc_nfc_add_template and oer_mc_nfc_get_source

Conditions: This symptom occurs on oer_mc_nfc_add_template and oer_mc_nfc_get_source.

Workaround: Change the border IP address.

- CSCti31984

Symptoms: Router crashes.

Conditions: This symptom occurs when “Show stats” is used to show auto Ethernet monitor operation.

Workaround: There is no workaround.

- CSCti32641

Symptom: A Cisco ASR 1004 (RP2) router is not able to establish an LDP session to a 3rd-party device and receives an Error Notification (0x07) Bad TLV Length message from that device.

Conditions: This symptom is observed on a Cisco ASR 1004 with Cisco IOS Release 15.0(1)S when LDP ICCP capability TLV (0x405) is supported on the router.

Workaround: There is no workaround.

Further Problem Description: It seems that Cisco ASR 1004 routers send to the peer a malformed ICCP capability TLV (0x405).

- CSCti34396

Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

Conditions: The symptom is seen when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10 match source-protocol static set ip
next-hop <router ip address> ! router bgp <asn> address-family ipv4 vrf <vrf name>
redistribute static route-map static-nexthop-rewrite exit-address-family exit exit
```

Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

For example, if you had:

```
ip route x.x.x.x 255.255.255.0 y.y.y.y
```

And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

```
ip route x.x.x.x 255.255.255.0 interface serial2/0
```

Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration “set ip next-hop self” is added to route-maps.

When used in conjunction with the newly added configuration:

```
router bgp <asn> address-family vpnv4 unicast bgp route-map priority
```

The “set ip next-hop self” will override “next-hop unchanged allpaths” for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34968

Symptoms: ACL with QoS is crashing the router, if one of the ACEs is evaluate or reflect.

Conditions: The symptom is observed if the pure ACL used under a class-map is also a reflexive ACL. It is observed only in a pure QoS class-map configuration which has only access-group match filter. It is not seen with an impure QoS class-map configuration which has access-group as well as other filters like DSCP.

Workaround: Do not use reflexive ACL under QoS. It is not a good practice.

- CSCti36310

Symptom: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attributes are pulled by SNMP.

Conditions: This symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

Workaround: There is no workaround.

- CSCti36423

Symptoms: Cisco IOS ASR router memory leaks when NHRP, SNMP, and DMVPN are configured.

Conditions: This symptom is observed in Cisco IOS ASR routers running the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S image.

Workaround: There is no workaround.

- CSCti39902

Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

Conditions: Configure RRI on the UUT.

Workaround: There is no workaround.

- CSCti40660

Symptoms: The following message is seen:

```
%FW-4-GLOBAL_SESSIONS_MAXIMUM: Number of sessions for the firewall exceeds the
configured global sessions maximum value 2147483647
```

Conditions: This symptom is observed when IP SLA is configured along with self zones

Workaround: Do not configure these features together.

- CSCti49472

Symptoms: System “accounting off” record is seen with suppress-CLI enabled.

Conditions: This symptom is observed with AAA CLI for suppressing system accounting records on switchover enabled when “Accounting OFF” is sent from a Cisco 7600 router.

Workaround: There is no workaround.

- CSCti51145

Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

Conditions: In order to see this problem, ALL of the following conditions must be met:

- The non-reloading device must have a “neighbor x.x.x.x transport connection-mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”
- It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload
- When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages
- Both peers must be multisession capable
- “transport multi-session” must not be configured on either device, or enabled by default on either device
- “graceful restart” must not be configured

Workarounds:

1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.

4. Configure graceful restart using the command **neighbor x.x.x.x ha-mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day-one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS 12.2(33)SB-based releases if the Release 12.2(33)SB router is the one not reloading.

- CSCti59562

Symptoms: DHCP accounting stop does not clear IP initiated sessions and radius-proxy sessions.

Conditions: This symptom occurs when VRF mapping is being used.

Workaround: There is no workaround.

- CSCti61949

Symptoms: Unexpected reload with a “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti62801

Symptoms: When both Caller-ID (CID) and Call-Waiting (CW) features are enabled on SIP analog endpoint, repetitive Call-Waiting (CW) tone is not played every 10 seconds until call is answered.

Conditions: The symptom is observed with a SIP analog endpoint on IAD243x, when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features using SIP for the phone connected to the FXS port.

Workaround: There is no workaround.

- CSCti66076

Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

Condition: This symptom is observed under the following conditions:

- HSRP version 1 is the protocol that must be used
- Use HSRP with sub-interfaces on ES20 module
- Reload the ES20 module

Workaround: Change to HSRPv2, which is not exposed to the issue.

Alternate Workarounds:

1. Reconfigure HSRP on all subinterfaces

2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti66153

Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment is logging the following error:

%VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Selector checks.

Conditions: This symptom is observed when the following conditions are met:

- A Cisco 7200 series router with VSA in receive-only mode
- Keyserver in receive-only mode
- Other GM in passive mode (that is encrypting outbound traffic) sending traffic to the “inside” of the Cisco 7200
- Traffic matching a keyserver delivered crypto ACL matching L4 ports (e.g.: **permit tcp any any eq 23**).

Workaround: Relax any of the conditions above as follows:

1. Use VAM2+ instead of VSA
2. Use GETVPN ACL without l4 ports (e.g.: **permit ip any any**)
3. Have the Cisco 7200 in passive mode as well
4. Not using receive-only mode on the keyserver.

- CSCti67102

Symptoms: Tunnel disables due to recursive routing loop in RIB.

Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

Workaround: There is no workaround.

- CSCti67832

Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

Workaround: There is no workaround.

- CSCti68721

Symptoms: The output of **show performance monitor history interval <all | given #>** will appear to have an extra column part way through the output.

Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

Workaround: If the symptom occurs, repeat the command.

- CSCti69008

Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

Conditions: This symptom is observed with dampening configuration changes for VRFs.

Workaround: There is no workaround.

- CSCti69990

Symptoms: A router crashes after unconfiguring IPv6 and then reconfiguring.

Conditions: The symptom is observed only under the following specific conditions:

- Router has IPv6 configured on a number of interfaces
- Router has GLBP configured
- IPv6 configuration is removed from all interfaces and then re-applied.

Workaround: There is no workaround.

- CSCti75666

Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on a Cisco ISR gateway that is running Cisco IOS Release 12.4(24)T2.

Workaround: Convert the H.323 leg to SIP.

- CSCti77879

Symptoms: When the traffic to encrypt matches the first sequence of a crypto map, starting its crypto ACL with a deny statement, the traffic is dropped whether or not this deny statement is a subset of the permits contained in that crypto ACL or not.

Also, the limitation of 14 denies in an ACL due to the jump behavior does not seem to be present.

Conditions: The symptom is observed in a VSA installed in a Cisco 7200 series router that is running Cisco IOS Release 15.0(1)M3.

Workaround: There is no workaround.

Further Problem Description: As the configuration guide states, the **crypto ipsec ipv4-deny {jump | clear | drop}** command should help to avoid this problem, but this command is not available for the VSA, only for VPN SPA.

- CSCti79442

Symptoms: One-way voice.

Conditions: The symptom is observed on a Cisco AS5400 MGCP controlled by PGW, SIP to PSTN call, with echo cancellation enabled. You see the RTP RX/TX counters increment with the **show call active voice brief** command.

Workaround: Explicitly define the MGCP codec type: **mgcp codec g711ulaw packetization-period 20**.

- CSCti82141

Symptoms: The following symptoms are observed:

1. The “none” option will be missing in the **show run** output after “**ntp pps-discipline none inverted stratum <#value>**” is configured.
2. “Invalid input detected” error message will be thrown during the bootup and the configured “**ntp pps-discipline none inverted stratum <#value>**” will vanish after a reload.

Conditions: The symptom is observed when the “inverted” option is included in the “**ntp pps-discipline**” CLI.

Workaround: Configure the CLI without the “inverted” option.

- CSCti84762
Symptoms: Update generation is stuck with some peers held in refresh started state (SE).
Conditions: This is seen with peer flaps or route churn and with an interface flap.
Workaround: Do a hard reset of the stuck peers.
- CSCti85446
Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.
Conditions: The symptom is observed under the following conditions:
 1. Configure a nexthop static route with permanent keyword
 2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface)
 3. Change the configuration in such a way that nexthop is reachable
 4. Configure a new static route through the same nexthop IP address used in step 1.
 Workaround: Delete all the static routes through the affected nexthop and add them back.
- CSCti87502
Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.
Conditions: This symptom is observed when attempting to launch CP Express.
Workaround: A power cycle fixes the issue temporarily.
- CSCti88897
Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2) T1, the command **service-policy output QOS_CUST_BASIC_OUT** disappears when the router is reloaded or power cycled.
Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2)T1.
Workaround: There is no workaround.
- CSCti91036
Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Release 15.1(2)T.
Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Release 15.1(2)T.
Workaround: There is no workaround.
- CSCti93175
Symptoms: NAT router does not translate address of the last TCP ACK in the 3-way handshake.
Conditions: The symptom is observed with the following conditions:
 - VRF NAT is involved
 - “ip nat outside source translation” has to exist.
 - NAT flow-entries are disabled by **no ip nat create flow-entries**.
 Workaround: There is no workaround.
- CSCti95511
Symptoms: The command **no buffer header permanent** does not restore the default number of header buffers.

Conditions: This symptom is observed under the following conditions:

- Only when configuring header/fast switching buffers
- Buffers need to be created for this pool.

Workaround: Configure the buffer CLIs carefully. This issue could be avoided by:

1. Not configuring “buffer header permanent” with a high value when available memory is low.
2. Not configuring “no buffer header permanent” when the number of buffers in the free list is less than the minimum value.

- CSCti97810

Symptoms: A “%SYS-2-FREEBAD” memory traceback is seen on an HA router.

Conditions: The symptom is observed on an HA router approximately 3-4 minutes after loading the image on an HA router.

Workaround: There is no workaround.

- CSCti97896

Symptoms: A Cisco ISR router with 512MB of memory and iomem set to 25% may crash and hang at bootup.

Conditions: The symptom is observed when booting a Cisco IOS 15.0 image with iomem set at 25% and 512MB of RAM.

Workaround: Do not configure “memory-size iomem 25”. To restore from the hang you will need to physically reload the router, break to rommon, and issue the following rommon command:

iomemset smartinit. Check that you have smartinit enabled using the rommon command **meminfo** which would show you “Smart Init is enabled.”

- CSCti98219

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>

- CSCti98347

Symptoms: DMVPN Phase 3 traffic flows stop and do not recover when the primary spoke loses WAN connectivity. NHRP entry on hub router continues to try to use NHRP mapping to spoke router that goes offline.

Conditions: This symptom occurs on routers running the asr1000rp1-adventerprisek9.02.06.02.122-33.XNF2.bin. image. Primary DMVPN Phase 3 spoke goes offline or loses connectivity and the NHRP mapping on the hub router doesn't get updated.

Workaround: Clear IP route for the network(s) on the hub router.

Further Problem Description:

```

Hub3#sho ip route next-hop-override | section % + - replicated route, % - next hop
override
D % 10.2.1.0 [90/2588672] via xxx.xx.x.x, 19:07:03, Tunnel2 [90/2588672] via
xxx.xx.x.x, 19:07:03, Tunnel2 [90/2588672] via xxx.xx.x.x, 19:07:03, Tunnel2
[NHO][90/1] via xxx.xx.x.x, 19:52:03, Tunnel2 <----- This is Tunnel IP that is
shutdown.
Sho ip nhrp cache 10.2.1.0 10.2.1.0/24 via xxx.xx.x.x <----- Pointing to redundant
spoke - this one should be used. Tunnel2 created 00:22:21, expire 00:04:03 Type:
dynamic, Flags: router used NBMA address: 10.1.12.12

```

- CSCtj00039

Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using **clear ip route vrf xxx x.x.x.x**.

- CSCtj01235

Symptoms: A crash is seen when running the command **debug crypto isakmp** during ISAKMP profile selection. The crashinfo file shows that the crash is happening during MM_KEY_EXCH as it receives the certificate from the remote peer.

Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 15.0(1)S.

Workaround: There is no workaround.

- CSCtj04278

Symptoms: In a DMVPN setup that is running the code of Cisco IOS Release 15.1TPI15, it is possible that NHRP Registrations are not sent by the box. This is seen if crypto is not configured using tunnel protection.

Conditions: This symptom occurs when tunnel protection is not configured.

Workaround: perform a shut/noshut of the tunnel interface.

- CSCtj04672

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat>.

- CSCtj05198

Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PFR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

Conditions: This symptom is observed when there are two EIGRP router processes.

Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj05903
Symptoms: Some virtual access interfaces are not created for VT, on reload.
Conditions: This symptom occurs on scaled sessions.
Workaround: There is no workaround.
- CSCtj06302
Symptoms: Cisco IOS ASR1000 SBC box crashes when it is trying to configure “media-address pool ipv4” CLI under SBC against the XNF2 image.
Conditions: This symptom occurs when “media-address pool ipv4” CLI is configured.
Workaround: There is no workaround.
- CSCtj08368
Symptoms: Router software crash at process_run_degraded_or_crash.
Conditions: The symptom is observed when the allocated memory block is freed.
Workaround: There is no workaround.
- CSCtj10592
Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.
Conditions: The symptom is observed with a simple SVTI to DVTI connection.
Workaround: There is no workaround.
- CSCtj16291
Symptoms: Voice router crashes due to memory corruption.
Conditions: The symptom is observed when multiple SIP Register are received. The response causes a Send Error.
Workaround: There is no workaround.
- CSCtj17316
Symptoms: EIGRP flaps up and down in a large scale network, when there is a lot of data to be sent.
Conditions: In an EIGRP network that has a large number of peers on a single interface, EIGRP might stop sending data to peers. This causes a flap due to packets not being acknowledged.
Workarounds:
 1. Find the instability in the network and fix the interface
 2. Summarize more routes
 3. Change more routers to stub
 4. Upgrade to rel7 of EIGRP.
- CSCtj17545
Symptoms: Immediately after a switchover, the restarting speaker sends TCP-FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.
Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.
Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

```
template peer-session ce-v4 transport connection-mode passive
```

- CSCtj21696

Symptoms: The virtual access interface remains down/down after an upgrade and reload.

Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv NAME: "chassis", DESCR: "2801 chassis" PID: CISCO2801 , VID: V04 , SN:
FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet" PID: CISCO2801 ,
VID: V04, SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard" PID:
VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch" PID: HWIC-4ESW , VID: V01 , SN:
FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire" PID:
WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capacity" PID:
PVDM2-8 , VID: NA , SN: FOC09123CTB
```

Workaround: Do a shut/no shut on the serial interface.

- CSCtj24453

Symptoms: The following traceback is observed when **clear ip bgp *** is entered:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP Scanner", ipl= 0, pid= 549
with call stack 0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
0x403A4E84:bgp_scanner(0x403a4c50)+0x234
```

Conditions: This symptom is rarely observed, but can occur when **clear ip bgp *** is entered with a lot of routes and route-map-cache entries.

```
Router# show ip bgp sum
BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
main routing table version 1228001 604000 network entries using 106304000 bytes of
memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
cache entries using 4565920 bytes of memory
```

The **clear ip bgp *** command is not a very common operation in the production network.

Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj27251

Symptoms: A router may crash when modifying a QoS class-map.

Conditions: The symptom is observed when modifying a QoS class-map which is being referenced by two or more policy-maps while traffic is matching the class-map and traversing the router.

Workaround: Remove the policy-maps that match the class-map to be modified by issuing **no service-policy input/output policy-map name**, make changes to the class-map, then re-apply the policy-maps by issuing **service-policy input/output policy-map name**.

- CSCtj28747

Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj32574

Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

```
router eigrp 1 redistribute connected no redistribute connected
```

The **no redistribute connected** command is not being backed up to the standby.

Conditions: The symptom is observed with any redistribute-related commands.

Workaround: There is no workaround.

- CSCtj33003

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip>

- CSCtj35106

Symptoms: Spurious memory access seen:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x61CBC400z reading 0x70
%ALIGN-3-TRACE: -Traceback= 0x61CBC400z 0x631A1ABCz 0x63156BA0z 0x631A508Cz
0x631A5600z 0x62B75A10z 0xFFFFF95C0z 0xFFFFF95C0z
0x61CBC400:ipv6_enqueue(0x61cbc3dc)+0x24
0x631A1ABC:fw_dp_insp_send_rsts(0x631a00b8)+0x1a04
0x63156BA0:fw_dp_tcp_inactivity(0x631567ac)+0x3f4
0x631A508C:fw_dp_insp_handle_sis_idle_timeout(0x631a4c64)+0x428
0x631A5600:fw_dp_insp_handle_timer_event(0x631a554c)+0xb4
0x62B75A10:tw_notify(0x62b75944)+0xcc
```

Conditions: The symptom is observed with any self-generated IPv6 traffic.

Workaround: There is no workaround.

- CSCtj36521

Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38234

Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

Workaround: There is no workaround.

- CSCtj38346

Symptoms: Router crash is seen when configuring the **default transmit-interface** command.

Conditions: The symptom is observed with Cisco IOS interim Release 15.1(2.19)T.

Workaround: There is no workaround.

- CSCtj39558

Symptoms: Sub-interface queue depth cannot be configured.

Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

Workaround: There is no workaround.

- CSCtj40564

Symptoms: Cisco ASR 1000 router disallows incoming Internet Key Exchange (IKE) connection that matches a keyring. This issue occurs after the router is reloaded.

Conditions: This symptom occurs when a crypto keyring, which has a local-address defined as an interface, is used.

```
crypto keyring keyring_test pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted> local
address Loopback2104
```

Workaround: Use an IP address.

```
crypto keyring keyring_test pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted> local
address <ip address>
```

- CSCtj41194

Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6>.

- CSCtj41867

Symptoms: A Cisco 2900 Integrated Service router that is running Cisco IOS Release 15.1(2)T exhibits increased memory utilization over time.

Conditions: The symptom is observed when a Cisco 2900 Integrated Services router that is running Cisco IOS Release 15.1(2)T is configured as a branch router that has an VPN WAN connection, Quality Of Service (QoS) classification configured ("qos pre-classify"), and WAAS Express enabled on a several interfaces with MLPPP enabled.

Workarounds:

1. Disable QoS classification on VPN tunnel interface
2. Disable WAAS Express on VPN tunnel interface
3. Reduce the number of serial interfaces down to one.

Further Problem Description: The symptom is not observed when QoS classification is not configured or when MLPPP is not configured or when WAAS Express is not enabled.

- CSCtj47736

Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

Conditions: The symptom is observed when the neighbor is learned, then a max-service limit is added on an address family, then a shut/no shut is done on the interface.

Workaround: There is no workaround.

- CSCtj47829

Symptoms: A buffer leak is experienced with “traffic-export” configured.

Conditions: The issue seen when you export traffic to an interface and to an NME-APPRE-502-K9. All conditions are not completely known yet.

Workaround: Disable the traffic-export functionality, for example:

```
Traffic export configs ip traffic-export profile axp-netscout interface
Integrated-Service-Engine1/0 bidirectional mac-address 0080.8c00.0001
interface FastEthernet0/0.99 encapsulation dot1Q 99 ip address xxx.xxx.xxx.xxx
255.255.255.0 ip traffic-export apply axp-netscout
Remove the configs interface fa0/0.99 no ip traffic-export apply axp-netscout no ip
traffic-export profile axp-netscout
```

- CSCtj48629

Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC-1CE1T1-PRI.

Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtj48913

Symptoms: Track does not recognize when an HTTP IP SLA probe’s status changes to OK.

Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

Workaround: There is no workaround.

- CSCtj52077

Symptoms: Policy at subinterface is not accepted with CBWFQ.

Conditions: This symptom is observed when policy is used in Ethernet subinterface.

Workaround: There is no workaround.

- CSCtj53363

Symptoms: Router hangs and console does not respond indefinitely.

Conditions: The symptom is observed with the following conditions:

- AIM-VPN in ISR + ZBFW; or,
- A Cisco 2811/2821 Onboard VPN + ZBFW.

Once traffic starts, router hangs within minutes.

Workaround: If running a Cisco 2811/2821, use sw crypto + ZBFW.

Alternate Workaround: If running Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj55624

Symptoms: A Cisco router crashes upon entering the **show crypto ruleset** command.

Conditions: This symptom is observed when v6 crypto maps are configured.

Workaround: Do not enter the **show crypto ruleset** command.

- CSCtj56019

Symptom: Mibwalk dot1dBridge using mst context does not return correct info.

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtj61284

Symptoms: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

Workaround: There is no workaround.

- CSCtj61657

Symptoms: IO memory leak is seen followed by TCP no buffer logs:
 %SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0XXXXXXXXX, alignment
 xxx Pool: I/O Free: xxxx Cause: Not enough free memory Alternate Pool: None Free: 0
 Cause: No Alternate pool -Process= "Pool Manager"
 %TCP-6-NOBUFF: TTY0, no buffer available -Process= "SCCP Application", ipl= 0, pid=
 XXX

Conditions: The symptom is observed in the presence of VOIP phones using multicast applications with the **session protocol multicast** dial-peer configuration command.

Workaround: There is no workaround.

- CSCtj65553

Symptoms: The static route that is installed in the default table is missing.

Conditions: This symptom is observed after Route Processor (RC) to Line Card (LP) to Route Processor transition on a Cisco Catalyst 3000 series switching module.

Workaround: Configure the missing static route.

- CSCtj69577

Symptoms: When congestion occurs on a QoS-enabled output interface, output rate significantly decreases.

Conditions: The symptom is observed under the following conditions:

1. 3945E outbound interface is connected to 100M link
2. QoS (LLQ/Fair Queue) is configured on 3945E outbound interface
3. Congestion occurs on outbound interface.

Workaround: Reload the router.

Further Problem Description: This issue is resolved after a reload but the shutdown/no shutdown commands can cause the same issue.

- CSCtj69886

Symptoms: NTP multicast over multiple hops.

Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

Workaround: There is no workaround.

- CSCtj72730

Symptoms: If an Enhanced Interior Gateway Routing Protocol (EIGRP) **address-family** configuration command is removed, any redistribution commands that refer to that address-family should also be removed. This defect documents a case where the redistribution command is not removed.

Conditions: This issue occurs when the redistribution command is not removed after removing the corresponding EIGRP address-family configuration command.

Workaround: Manually remove the redistribution commands that remain after the **address-family** command is removed.

- CSCtj76297

Symptoms: Router hangs with interoperability of VM and crypto configurations.

Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

Workaround: Disable AIM and use onboard CE.

- CSCtj77004

Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

Conditions: The symptom is observed when “archive log config” is configured.

Workaround: There is no workaround.

- CSCtj77285

Symptoms: Router CPU becomes high tending towards 80%+ from normal operating conditions. The command **show mem | inc FNF OCE** will show multiple rows rather than just a couple of rows.

Conditions: The symptom is observed with voice calls and VOIP in use. It is seen when Flexible NetFlow is configured.

Workaround: Switch off Flexible NetFlow (although that leaves memory consumption in place and CPU higher than normal) or reboot the router.

- CSCtj77477

Symptom: High delay in priority queue when using CBWFQ/LLQ. For example:

```
EFM rate 2304 kbps
888E Average delay: 42ms 888E Max delay: 63ms HWIC-4SHDSL-E Average delay: 216ms
HWIC-4SHDSL-E Max delay: 361ms
```

Conditions: The symptom occurs only on Cisco G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface. For example:

```
EFM rate 2304 kbps
policy-map CHILD class voice priority percent 25 class business bandwidth percent 50
policy-map PARENT class class-default shape average 2100000 8400 0 service-policy
CHILD
```

- CSCtj77963

Symptoms: Resets are observed on low speed links.

Conditions: The symptom is observed on low speed interfaces over the WAN that produce retransmissions, out of order segments, etc.

Workaround: There is no workaround.

- CSCtj78966
Symptoms: A Cisco ASR router crashes with thousands of IKEv2 sessions, after numerous operations on the IKEv2 session.
Conditions: This symptom is observed when the IKEv2 SA DB WAVL tree is corrupted if we fail to insert the SA due to some error (for example, PSH duplication).
Workaround: There is no workaround.
- CSCtj79368
Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.
Conditions: The symptom is observed when removing RSA keys.
Workaround: Stay on the same RSA keys.
- CSCtj79750
Symptoms: Multicast responses are not obtained.
Conditions: This symptom is observed after a Multicast Listener Discovery (MLD) join.
Workaround: There is no workaround.
- CSCtj79769
Symptoms: An LC crashes.
Conditions: This symptom is observed during unconfiguration.
Workaround: There is no workaround.
- CSCtj81533
Symptoms: The following error message is seen:

```
np_vsmgr_modify_connection: invalid service id 11 passed
```


No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.
Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.
Workaround: There is no workaround.
- CSCtj82292
Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.
Conditions: This issue occurs when summary address is advertised as follows:

```
ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
```


Workaround: There is no workaround.
- CSCtj82387
Symptoms: Config sync @ pppoe server remote-id
Conditions: This symptom is observed on the Cisco 7600 platform with Cisco IOS Release_15.1(1.14)S.
Workaround: There is no workaround.
- CSCtj84901
Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

1. Service Ready Engine modules (ISM and SM SRE)
2. Etherswitch modules (SM and EHWIC)

If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj85333

Symptoms: System may crash when config-template contains the config command **ip ips signature-category** and when the template is downloaded to the router using the CNS config feature commands **cns config retrieve** (exec command) and **cns config initial** (config command). This symptom may also occur when the config template is downloaded to the router using the device Config-Update operation of Config Engine.

Conditions: This symptom is observed in normal mode operation, but will also occur when the CNS feature is used.

Workaround: There is no workaround.

- CSCtj87180

Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of "SSS Manager Disconnected Session".

Conditions: The symptom is observed when the LAC router receives the following message from the multihop peer:

```
"Error code(9): Try another directed and Optional msg: SSS Manager disconnected
session <<<< INVALID"
```

Workaround: There is no workaround.

- CSCtj89941

Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

Conditions: The symptom is observed under the following conditions:

1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured
2. Use IXIA to generate 1Gbps traffic
3. Wait until all the SAs have been established and traffic is stable
4. Use CLI **clear crypto session** on EzVPN simulator.

Workaround: There is no workaround.

- CSCtj90438

Symptoms: Router crashes if “no switchport” is executed on /1 interface of Enhanced Etherswitch (ESW) or Service Ready Engine (SRE) module.

Conditions: This symptom occurs while executing “no switchport” on the /1 interface of ESW or SRE module without HWIC-4ESW, HWIC-D-9ESW, HWIC-4ESW-POE, HWIC-D-9ESW-POE, NM-16ESW, and NM-16ESW-1GIG present.

Workaround: Do not execute the **no switchport** command on the above mentioned modules as this command does not apply to these modules.
- CSCtj91190

Symptoms: Non-queue same direction policy is not getting accepted.

Conditions: This symptom is observed on post HQF images when the policy is used on both the ATM main and sub interfaces.

Workaround: There is no workaround.
- CSCtj91764

Symptoms: A Cisco UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

Conditions: This symptom is observed during a complete SNMP MIB walk.

Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.
- CSCtj92692

Symptoms: Path-confirmation failure seen with rtp-nte to out-of-band dtmf interworking.

Conditions: This symptom is observed with the following setup:

```
Callgen---OGW---H323---CUBE---H323---TGW---Callgen
```

Workaround: Configure rtp-nte end to end.
- CSCtj94297

Symptoms: “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

Workaround: Use the **clear ip mroute** in the affected mroute.
- CSCtj94617

Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

Conditions: This symptom is observed when issuing the **show running** command.

Workaround: There is no workaround.

Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.
- CSCtj97823

Symptoms: The 32-byte topology names are not handled correctly on bootup.

Conditions: This symptom occurs when 32-byte topology names are not handled correctly on bootup.

Workaround: Use topology names shorter than 32 characters.

- CSCtk02515
Symptoms: Path confirmation fails for a basic call between SCCP and SIP endpoints.
Conditions: This symptom is observed with Cisco IOS Release 15.1(3.7)T.
Workaround: There is no workaround.
- CSCtk02547
Symptoms: Informer router reloads @ __be_gige_dsp_handle_voice_queue.
Conditions: This symptom is observed on a Cisco router running a Cisco IOS 151-3.7.T image.
Workaround: There is no workaround.
- CSCtk02647
Symptoms: On an LNS configured for L2TP aggregation, it might be that per-user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).
Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.
Workaround: There is no workaround.
- CSCtk02666
Symptoms: During a graceful restart event, the peer undergoes reconfiguration. This may result in stale labels on the RRP.
Conditions: The symptom is observed with GR + SSO + peer reprovisioning.
Workaround: Perform a **clear xconnect** or flap the local VC.
- CSCtk06548
Symptoms: Using CCBU CVP solution, SIP calls are disconnected during stress test.
Conditions: The symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by SIP stack. It is seen with PI14 image testing.
Workaround: Use PI12 image.
Further Problem Description: The fundamental issue involves the selective ack (SACK) feature. An alternative workaround would be to disable the “SACK Permitted” option from the peer.
- CSCtk07576
Symptoms: Routers reload while configuring the “station-role root.”
Conditions: This symptom is observed while configuring the “station-role root” in the uclient with ssid killers.
Workaround: There is no workaround.
- CSCtk10279
Symptoms: A router configured for LISP may crash if it receives a LISP Map-Reply message with an IPv6 RLOC, when IPv6 routing is not enabled.
Conditions: This symptom occurs when LISP is configured using the **ip lisp {itr | etr | proxy-itr | proxy-etr }** command, the router does not have IPv6 routing configured using the **ipv6 unicast-routing** command.
Workaround: Enable the IPv6 routing by entering **ipv6 unicast-routing** command.
- CSCtk12122
Symptoms: A Cisco 7200 router may crash after clearing the SAs while using IKE keepalive feature.

Conditions: This symptom is observed when the IKE keepalive feature is turned on and the user executes a “clear crypto session” or “clear crypto sa.”

Workaround: There is no workaround.

- CSCtk12608

Symptoms: Route watch fails to notify the client when an RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, Release 15.1(2)T and Release 15.1(01)S and with the following configurations:

```
Router 1: interface Ethernet0/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx !
interface Ethernet1/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! router bgp 100 no
synchronization bgp log-neighbor-changes neighbor xxx.xxx.xxx.xxx remote-as 200 neighbor
xxx.xxx.xxx.xxx ebgp-multihop 255 no auto-summary !

ip route 0.0.0.0 0.0.0.0 10.10.200.1 ip route xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx 10.0.12.2 ip route
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx

Router 2: interface Loopback200 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! interface
Loopback201 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! interface Ethernet0/0 ip address
xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx !

interface Ethernet1/0 ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx ! router bgp 200 no
synchronization bgp log-neighbor-changes network xxx.xxx.xxx.xxx neighbor xxx.xxx.xxx.xxx
remote-as 100 neighbor 10.0.12.1 update-source Loopback201 no auto-summary ! ip route 0.0.0.0
0.0.0.0 xxx.xxx.xxx.xxx !
```

Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12681

Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk15360

Symptoms: Xauth userid mode http-intercept does not prompt for a password and the EzVPN session does not come up.

Conditions: This symptom occurs when the EzVPN client x-auth is configured as http-intercept.

Workaround: There is no workaround.

- CSCtk15410

Symptoms: Spurious memory access is seen at rmon_int_command.

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtk16310

Symptoms: Timeout failure occurs due to “No socket” error.

Conditions: This symptom occurs with Udp-jitter packet with VRF.

Workaround: There is no workaround.

- CSCtk18607

Symptoms: Router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

Conditions: This symptom occurs at `ssh_pubkey_command_nvgen` and `ssh_pubkey_nvgen`.

Workaround: There is no workaround.

- CSCtk31401

Symptoms: A Cisco router crashes when the SSH session from it is exited.

Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

Workaround: There is no workaround.

- CSCtk35650

Symptoms: Router hangs while generating IP SLA auto schedule with maximum length.

Conditions: This symptom occurs while generating IP SLA auto schedule.

Workaround: There is no workaround.

- CSCtk36891

Symptoms: Video conferencing through NAT may crash the router.

Conditions: This symptom is observed when NAT is configured. Video conferencing with PVDM3 crashes the router.

Workaround: Remove NAT configurations.

- CSCtk37395

Symptoms: A Cisco 2921 cannot process fax calls and reports the following:

```
%MSPI-1-NOMEMORY: Unit 770, no memory for mspi_on_xmit, disconnect connection
```

Conditions: Conditions are not known. The symptom may occur when the processor's free memory is more than 4GB/6.

Workaround: Reduce slightly the processor memory while increasing the i/o memory and see if this is indeed what is causing the problem:

- The command is “memory-size iomem 25” on systems with more than 1Gb
- On systems with 1Gb io mem, you cannot take more than 10%. Instead, use logging buffer 200Mb to decrease free processor memory. This workaround helps to mitigate the issue.

- CSCtk46363

Symptom: A device running Cisco IOS and acting as a DHCP server crashes.

Conditions: This symptom is observed when a client requests a specific IP address.

Workaround: Disable duplicate address detection check using the **`ip dhcp ping packet 0`** command.

- CSCtk53130

Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

```
Incompatible with ipv6 command on Vp1 - command rejected.
```

Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

Workaround: There is no workaround.

- CSCtk54830

Symptom: ARP entry is removed from the ARP table by DHCP.

Conditions: This symptom is observed when replying back to the client Request/Inform.

Workaround: There is no workaround.

- CSCtk56570

Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.

Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

Workaround: Disable media transcoder-high-density.

- CSCtk58732

Symptoms: The router may crash if the following configuration is applied:

```
ip sla 1 icmp-jitter xxx.xxx.xxx.xxx source-ip xxx.xxx.xxx.xxx num-packets 1 interval
10 threshold 1000 timeout 1000 frequency 10
ip sla schedule 1 start-time now life forever
```

```
track 1 ip sla 1 reachability
```

The following error message is displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 10:49:31 UTC Mon Feb 21 2011 addr=0x1,
pc=0x62D97F30z , ra=0x62D98848z , sp=0x67CE34D0
10:49:31 UTC Mon Feb 21 2011: Address Error (store) exception, CPU signal 10, PC =
0x62DA2E10
```

Conditions: This symptom is observed in Cisco IOS Release 15.1(3)T. The router may continually reload following the crash.

Workaround: Use the ICMP Echo operation instead, as shown below:

```
ip sla 1 icmp-echo 192.0.2.1 source-ip 192.0.2.2 threshold 1000 timeout 1000 frequency
10
```

- CSCtk61069

Symptoms: The Cisco IOS router crashes.

Conditions: This symptom occurs while entering “write memory” or “show running configuration” on the router after configuring “privilege exec level 15 show adjacency.”

Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62247

Symptoms: IKEv2 session fails to come up with RSA sign authentication.

Conditions: The symptom is observed with a hierarchical CA server structure.

Workaround: Use non-hierarchical CA servers.

- CSCtk62626

Symptoms: Memory leak could be observed after 802.1X or MAB authentication when using VLAN and DHCP assignment.

Conditions: This symptom is observed on a Cisco 890 router configured for 802.1X authentication.

Workaround: There is no workaround.

- CSCtk67073

The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla>.

- CSCtk68647

Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk74970

Symptoms: TE autoroute announced tunnel is not installed in the routing table.

Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute announced tunnel is not installed in the routing table.

Workaround: Configure “no ip routing protocol purge interface”.

- CSCtk83638

Symptoms: A client is assigned an ip address from an incorrect pool when it reconnects with a different profile.

Conditions: This symptom is observed in a setup where two clients are behind an NAT router. When one client’s connection is broken, the server is not made aware of this, then the client reconnects with a different group, the IP address assigned is not from the correct pool.

Workaround: There is no workaround.

- CSCtk84116

Symptoms: A GETVPN ks crash may occur.

Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

Workaround: There is no workaround.

- CSCtk98726

Symptoms: ANCP shaper fails to be applied on ATM VC.

Conditions: This symptom occurs after clearing and re-establishing the PPPoE session.

Workaround: There is no workaround.

- CSCtl00467

Symptoms: A Cisco router crashes while using conference call.

Conditions: This symptom is observed when the conference call feature is used.

Workaround: There is no workaround.

- CSCtl04285

Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

Conditions: The symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are Cisco IOS Release 12.2(33)SRE, Release 15.0M, Release 12.2(33)XNE, and later releases.

- Workaround: There is no workaround.
- CSCtl05941

Symptoms: CUBE crashes.

Conditions: This symptom is observed when voice HA is configured on CUBE.

Workaround: There is no workaround.
 - CSCtl67195

Symptoms: The following three BGP debug commands are not allowed to enable:

debug ip bgp vpnv4 unicast
debug ip bgp vpnv6 unicast
debug ip bgp ipv6 unicast

Conditions: The symptom is observed with the above BGP debug commands.

Workaround: There is no workaround.
 - CSCtl71478

Symptoms: In an HA system, the following error message is displayed on the standby RP and LC:

"OCE-DFC4-3-GENERAL: MPLS lookup unexpected"

Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

Workaround: There is no workaround.
 - CSCtl74163

Symptoms: Some PPPoEoA PVCs that are configured with Auto VC feature may fail to disconnect after idle timeout timer expires.

Conditions: The issue is observed on Cisco IOS ASR1006 router when the traffic generator creates 4000 PPPoEoA sessions for every ATM interface.

Workaround: Perform shut and no shut to clear the VCs.
 - CSCtl77735

Symptoms: Saving a configuration to NVRAM may fail.

Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

Workaround: Erasing the startup configuration and saving again may recover the configuration.
 - CSCtl87067

Symptoms: Priority class will drop traffic before explicit police rate is reached.

Conditions: This symptom is observed on Cisco ISR platforms when strict priority with explicit police is configured.

Workaround: There is no workaround.
 - CSCtl87879

Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

Workaround: There is no workaround.

- CSCtl88066

Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

Conditions: The symptom is observed when BGP is configured and you issue one of the following commands:

```
show ip bgp all attr nexthop
show ip bgp all attr nexthop rib-filter
```

Workaround: Do not issue either of these commands with the “all” keyword. Instead, issue the address-family specific version of the command for the address family you are interested in.

For example, the following are safe:

```
show ip bgp ipv4 unicast attr nexthop
show ip bgp attr nexthop
show ip bgp vpnv4 vrf vrfname attr nexthop
```

Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing, and where this fix is not integrated are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl92210

Symptoms: A Cisco router may crash when trying to show the session objects while session queue is being managed (addition/removal).

Conditions: This symptom is observed when new sessions are being provisioned or removed from mediatrace initiator side. The router may crash when trying to show the session objects while the session queue is being managed (addition/removal) or when the **no mediatrace responder** command is entered.

Workaround: User can only avoid using show “mediatrace responder sessions” command if additions or removals are being done at Mediatrace responder node.

- CSCtl98270

Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

Conditions: The symptom is observed in Cisco IOS Release 15.1(2)T2 and later releases.

Workaround: Execute a shut/no shut to fix the issue.

- CSCtn01047

Symptoms: Firewall service-policy attachment failed.

Conditions: This symptom is observed with Zone Based Firewall.

Workaround: There is no workaround.

- CSCtn01832

Symptoms: The following command sequence crashes the router at check syntax mode:

```
config check syntax route-map hello match local-preference no match local-preference
```

Conditions: The symptom is observed with the commands above.

Workaround: There is no workaround.

- CSCtn09135
Symptoms: MC5728V modem is not enumerated resulting in cellular interface not coming up.
Conditions: This symptom occurs more often with USB flash attached and on DSL SKUs versus non-DSL SKUs.
Workaround: Removing the USB flash solves the issue in some instances.
- CSCtn10922
Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic and in some cases may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.
Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.
Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.
- CSCtn21154
Symptoms: A crash occurs at mace_dp_update_post_mace_metrics.
Conditions: This symptom is observed when MACE and NAT are configured together.
Workaround: Do not configure NAT along with MACE.
- CSCtn27599
Symptoms: The OIR of NM-1T3/E3 line card crashes the router.
Conditions: This symptom is observed only on the Cisco 3945 router.
Workaround: There is no workaround.
- CSCtn37743
Symptoms: Egress interface is not correct as observed by Mediatrace responder. This can impact monitoring on perf-traffic and system profiles.
Conditions: This symptom is observed on a node where it has both initiator and responder, when the responder has both high and low cost routes and when the interface is changed, the change is detected but the egress is not reflected.
Workaround: Remove the original session and re-add it.
- CSCtn39632
Symptoms: An RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.
Conditions: This symptom is observed on a Cisco ASR router configured for RSA key encryption with a keyring name having more than 8 characters.
Workaround: Modify the keyring name to be less than 8 characters.
- CSCtn46263
Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.
Conditions: This symptom is observed during retransmissions and window throttling of requests.
Workaround: There is no workaround.
- CSCtn51740
Symptoms: Memory leak is seen in EzVPN process.

Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

Workaround: There is no workaround.

- CSCtn54985

Symptoms: The status of a LSP health monitor with LSP discovery is shown as “unknown.”

Conditions: This symptom is observed on “PE” routers in an MPLS VPN scenario when configured with LSP health monitors.

Workaround: There is no workaround.

- CSCtn55187

Symptoms: Memory leaks are seen at `ikev2_ipsec_add_proxy_to_list`, `ikev2_skeyseed_create` and `ikev2_ios_get_ipv6_pak` on Cisco 2900 and 3900 platform router, respectively.

Conditions: This symptom is observed on Cisco 2900 and 3900 platform routers.

Workaround: There is no workaround.

Further Problem Description: Memory leaks are seen after the test has been completed and while trying to check for the memory leaks while testing the feature Tunnel Protection for IPv6 feature.

- CSCtn66356

Symptoms: Sometimes AP802 Radio module may not be recognized by the AP IOS running on the second CPU core.

Conditions: Conditions are not known at this time.

Workaround: There is no workaround.

- CSCtn69929

Symptoms: The DHCP Server will not assign any addresses to clients, even though Smart-install is configured with DHCP pool parameters.

Conditions: This symptom is observed when Smart-install is configured to assign DHCP addresses.

Workaround: Execute “show running-config” on the box once; after that, everything works fine.

- CSCtn74169

Symptoms: Crash by memory corruption occurs in the process “EzVPN Web-intercept daemon.”

Conditions: This symptom is observed with an EzVPN connection coming up after HTTP authentication using HTTP Intercept.

Workaround: Do not use HTTP Intercept.

- CSCtn77154

Symptoms: The Stateful Inspection Feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets punted to the CPU. This results in overall performance degradation.

Conditions: This symptom is observed when two outside NAT interfaces are configured.

Workaround: Configure “ip nbar protocol discovery.”

- CSCtn84628

Symptoms: A Cisco CGR2010 reports an over-temperature error message when the system is running in a 60C environment.

Conditions: This symptom is observed when the environment is at 60C.

Workaround: Ignore the error message from the sys log.

- CSCto00318

Symptoms: An SSH session initiated from a router running Cisco IOS 15.x releases may cause the router to reboot.

Conditions: This symptom is observed with Cisco IOS 15.x releases.

Workaround: Do not initiate SSE sessions; otherwise, there is no workaround.

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.1T. These documents consist of software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Use these release notes with the documents and tools described in the following sections:

- [Cisco Feature Navigator, page 747](#)
- [Cisco IOS Software Documentation Set, page 747](#)

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is available 24 hours a day, 7 days a week, and is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/cfn>

Cisco IOS Software Documentation Set

The Cisco IOS Release 15.1T documentation set consists of configuration guides, command references, and other supporting documents and resources. For the most current documentation, go to the following URL:

http://www.cisco.com/en/US/products/ps10592/tsd_products_support_series_home.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
 "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 747.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2010-2013 Cisco Systems, Inc.
All rights reserved. Printed in USA.