



Caveats for Cisco IOS Release 12.4

September 11, 2012

Cisco IOS Release 12.4(25g)

Text Part Number OL-7656-15 Rev. J0

This document lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.4, up to and including Cisco IOS Release 12.4(25g). Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

To improve this document, we would appreciate your comments. If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically at <http://www.cisco.com/feedback/> or contact caveats-doc@cisco.com. For more information, see the “Obtaining Documentation and Submitting a Service Request” section on page 980.

Contents

- [How to Use This Document, page 3](#)
- [Field Notices and Software-Related Tools and Information, page 4](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25g\), page 4](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25f\), page 6](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25e\), page 9](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25d\), page 12](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25c\), page 21](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25b\), page 39](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25a\), page 46](#)
- [Open Caveats—Cisco IOS Release 12.4\(25\), page 48](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(25\), page 53](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(23b\), page 81](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(23a\), page 82](#)



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

- [Resolved Caveats—Cisco IOS Release 12.4\(23\), page 97](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(21a\), page 126](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(21\), page 127](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(19b\), page 158](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(19a\), page 158](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(19\), page 161](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(18e\), page 174](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(18c\), page 177](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(18b\), page 182](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(18a\), page 186](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(18\), page 196](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(17b\), page 216](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(17a\), page 223](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(17\), page 231](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(16b\), page 259](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(16a\), page 279](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(16\), page 288](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13f\), page 314](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13e\), page 318](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13d\), page 330](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13c\), page 334](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13b\), page 338](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13a\), page 343](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(13\), page 346](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(12c\), page 373](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(12b\), page 375](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(12a\), page 381](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(12\), page 390](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(10c\), page 416](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(10b\), page 426](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(10a\), page 437](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(10\), page 443](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(8d\), page 479](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(8c\), page 494](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(8b\), page 500](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(8a\), page 508](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(8\), page 519](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7h\), page 568](#)

- [Resolved Caveats—Cisco IOS Release 12.4\(7g\), page 570](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7f\), page 571](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7e\), page 578](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7d\), page 584](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7c\), page 598](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7b\), page 604](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7a\), page 619](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(7\), page 632](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(5c\), page 670](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(5b\), page 695](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(5a\), page 709](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(5\), page 719](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3j\), page 774](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3i\), page 775](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3h\), page 777](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3g\), page 783](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3f\), page 789](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3e\), page 794](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3d\), page 798](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3c\), page 807](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3b\), page 810](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3a\), page 821](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(3\), page 823](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(1c\), page 899](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(1b\), page 904](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(1a\), page 930](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(1\), page 939](#)
- [Obtaining Documentation and Submitting a Service Request, page 980](#)

How to Use This Document

This document describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The “Open Caveats” section lists open caveats that apply to the current release and may apply to previous releases.
- The “Resolved Caveats” sections list caveats resolved in a particular release, but open in previous releases.

Within the sections, the caveats are sorted by technology in alphabetical order. For example, Interfaces and Bridging caveats are listed separately from, and before, IP Routing Protocols caveats. The caveats are also sorted alphanumerically by caveat number.

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.

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/web/download/index.html> or by logging in to Cisco.com and selecting **Support > Download Software**.



Note

Release notes are modified only on an as-needed basis. The maintenance release number and the revision date represent the last time the release notes were modified to include new or updated information. For example, release notes are modified whenever any of the following items change: software or hardware features, feature sets, memory requirements, software deferrals for the platform, microcode or modem code, or related documents.

The most recent release notes when this caveats document was published were [Release Notes for Cisco IOS Release 12.4](#), for Cisco IOS Release 12.4(25), on April 24, 2009.

Resolved Caveats—Cisco IOS Release 12.4(25g)

Cisco IOS Release 12.4(25g) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25g) but may be open in previous Cisco IOS releases.

- CSCsv05430

Symptoms: DATACORRUPTION-1-DATAINCONSISTENCY is seen when DSP sends an alarm indication with 80 words of content.

Conditions: DSP sends an alarm indication message that is 80 words of content due to abnormal condition or error condition. Shorter alarm message will not trigger DATACORRUPTION-1-DATAINCONSISTENCY message.

Workaround: There is no workaround.

- CSCtc42278

Symptoms: The following error message is seen for incoming ISDN calls:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

This error should be cosmetic and not service impacting.

Conditions: This symptom is observed on a Cisco AS5400XM with ISDN configured. Also applies to newer versions of Cisco IOS Releases 12.4T, 15.0M&T, 15.1M&T.

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

- CSCtg48785

Symptoms: The following error may appear in the log:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
```

Conditions: This issue occurs while issuing **show x25 hunt- group** command when a large amount of x25 traffic has passed through the hunt-group member element.

Workaround: Do not use the **show x25 hunt-group** 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>

- CSCtj48387

Symptoms: After a few days of operation, a Cisco ASR router that is 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.

Further Problem Description: This fix needs to be included in the Cisco ME 3400.

- 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>

- 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.

- 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>

- 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>

- 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>

- CSCub84274

Symptoms: Every alternate ping is dropped.

Conditions: Pings over the tunnels are dropped.

Workaround: Enable “debug dialer cef”.

Resolved Caveats—Cisco IOS Release 12.4(25f)

Cisco IOS Release 12.4(25f) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25f) but may be open in previous Cisco IOS releases.

- CSCsl11129

Symptoms: A Cisco IOS device configured with Cisco IOS Gateway for T.37 On-Ramp Fax Support may crash with a bus error.

Conditions: This symptom is seen when the device is configured for the following:

1. Cisco IOS Gateway for T.37 On-Ramp Fax Support.
2. The combination of both the configured **hostname** and **ip domain-name** has characters exceeding 50 characters.

Workaround: Reduce the size of the hostname.

- CSCsz39222

Symptoms: The Cisco CMTS reloads and crash file indicates a cache error.

Conditions: This issue is observed when register 26/0 contains 0xC0000000.

This issue affects the NPE-G1 on a Cisco 7200 platform, and the PRE4 on a Cisco UBR10012 router. NPE-G2 is not affected. There is no specific trigger for this failure other than having a single bit parity error on ECC memory.

Workaround: There is no workaround.

Further Problem Description: This symptom does not cause a parity error or actually cause the crash. This symptom is just to add a error handler for the specific case of a single bit correctable parity error in ECC memory. The crash results from the parity error itself. The following is an example of the beginning of a crashinfo collection for a hardware corrected cache error:

```
Cache error detected!
CPO_ECC      (reg 26/0): 0xC0000000
CPO_CACHERI  (reg 27/0): 0x34001DE0
CPO_CACHERD  (reg 27/1): 0x10800580
CPO_CCHEDPA  (reg 27/3): 0x017B4580
```

- 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.

- 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://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml>.

- CSCth87458

Symptoms: Memory leak is detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

Conditions: This is 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

- 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://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml>.

- 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.

- CSCto88178

Symptoms: Packet corruption is observed when NAT processes an H.323 packet that has some trailing data beyond the User-User Information Element.

Conditions: This symptom occurs when NAT is configured to process H.323 packets, and it encounters an H.323 packet that has some trailing data beyond the User-User Information Element.

Workaround: Although it is not feasible for most implementations, using the **no ip nat service H225** command prevents the packet corruption. Additionally, this issue is not present in those releases that have NAT TCP ALG support enabled.

- CSCtr29202

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 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 when 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.

- 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>

Resolved Caveats—Cisco IOS Release 12.4(25e)

Cisco IOS Release 12.4(25e) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25e) but may be open in previous Cisco IOS releases.

- CSCsk46486

Symptoms: The Gigabit controller of NPE-G2 board does not correctly recognize the QinQ encapsulation, dropping the packets as giants. The packets with double encapsulation above 1496 bytes are not passing through, being dropped at the input of the NPE-G2 as giants. Reverting to single encapsulation on both sides, the behavior returns as expected, allowing the ping with any size.

Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.2(31)SB7.

Workaround: Configure the L2 interface MTU to 1504 instead of 1500.

- CSCsl24511

Symptoms: The problem was introduced due to the existence of multiple outgoing mcast interfaces. When ToS was changed from one interface during particle-based fastswitching, the change was carried to other interfaces, which made QoS policy perform incorrectly.

Conditions: Fix should be applied to Cisco IOS Releases 12.2SR and 12.2SX. The reported issue is not seen haw_t, however, since it will fix CSCtj49957 which was duplicated to this DDTS, this fix should also be committed to t-train, and all other major branches which is NOT using MFIB forwarding.

Workaround: Disable fastswitching and do process switching only.

- CSCsx98284

Symptoms: A router may crash with a bus error and with a corrupted program counter:

```
%ALIGN-1-FATAL: Corrupted program counter pc=0x66988B14 , ra=0x66988AFC ,
sp=0x66A594D0
```

Conditions: The symptom is observed on a Cisco IOS Voice over IP (VOIP) gateway configured for IPIPGW (CUBE) as well as Cisco Unified Communications Manager (CUCM) controlled MTP on the same gateway. Under situations where a call loop is present (same call routing back-forth through the same gateway), the system may reload if an MTP is also present in the loop.

Workaround: Find and break the source of the call loop. Be careful of default destination-pattern/route-patterns that may kick in under some conditions.

Alternate workaround: Separate the MTP functionality from the gateway.

- CSCsz88850

Symptoms: Active RPs CPU% spikes by MLD process/PIM process after reload or switchover or interface state flapping.

Conditions: This MLD CPU spike is seen right after the bootup when active RP is synching with standby RP. The PIM CPU spike is seen when the interface state is changing. These two problems are seen randomly.

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://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml>.

- 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.

- 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://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml>.

- CSCth95192

Symptoms: On a Cisco router loaded with Cisco IOS Release 12.0(33)S6, when LSP changes, the CEF table may become stuck with old label information.

Conditions: This symptom occurs when there are two outgoing links to the BGP next hop for the prefix received via BGP.

The following is a snapshot of how the CEF table will be during the time of the issue:

```
R1# show ip cef 10.150.150.150 detail
```

```

10.150.150.150/32, version 26, epoch 0, cached adjacency 10.1.15.5
0 packets, 0 bytes
  tag information from 10.100.100.0/30, shared, all rewrites owned
    local tag: 33
    fast tag rewrite with Et0/0.12, 10.1.1.1, tags imposed {16}
  via 10.100.100.2, 0 dependencies, recursive
    next hop 10.1.15.5, Ethernet0/0.15 via 10.100.100.0/30 (Default)
    valid cached adjacency
    tag rewrite with Et0/0.15, 10.1.15.5, tags imposed {502}

```

Workaround: Issue the **clear ip route** command.

- 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

- 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.

- 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 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.

- 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.

- CSCtn77090

Symptoms: Gradual increase of CPU with CPU topping at 99% and increase in holding memory for IP SLA process may cause crash on routers that are running IP SLA probes, generally above 300 probes.

Conditions: This symptom is observed when there are more than 20 SNMP simultaneous probe restarts from IP SLA management software.

Workaround: Limit SNMP probe restarts to under 20 from IP SLA management software.

Resolved Caveats—Cisco IOS Release 12.4(25d)

Cisco IOS Release 12.4(25d) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25d) but may be open in previous Cisco IOS releases.

- CSCee93607

Symptoms: A VPN client cannot connect to a router that functions as an EzVPN server.

Conditions: This symptom is observed on a Cisco router that functions as an EzVPN server when the username is not sent in the RADIUS authentication request for the VPN client, causing the authentication server to reject the VPN client.

Workaround: Use local authentication if this is an option.

Further Problem Description: The following error message appears in the debug output:

```
ISAKMP (0:1): FSM action returned error: 4
```

- CSCsg39977

Symptom: When dialer interfaces are used in conjunction with Multilink PPP (MLP), a router may crash because of a corrupted program counter.

Conditions: This symptom is observed on a Cisco router when a dialer interface, including interfaces such as ISDN BRI and PRI interfaces, is configured to use MLP and when the queueing mode on the dialer interface is configured for Weighted Fair Queuing (WFQ). Note that WFQ is the default for some types of dialer interfaces.

Workaround: There is no workaround.

- CSCsk55161

Symptoms: Cisco IOS software crashes when enabling multicast feature of scaled-up configuration.

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.

- CSCsv22754

Symptoms: The default originate route is not getting withdrawn when a peer template is used on a neighbor.

Conditions: Configure default-originate in the peer template (say ptemp) and apply it on the neighbor; then the default route will be advertised to the neighbor. But when you remove this configuration on ptemp, the route will not be withdrawn.

Workaround: Enter the following command:

clear ip bgp * soft in

- CSCsv81176

Symptoms: A router crashes with syslog CHUNKBADMAGIC.

Conditions: This symptom is observed with an ATM interface and a NAT outside interface on a Cisco 3845 platform. It has been seen with a large number of flows from thousands of source addresses and with thousands of translated source addresses in a short period of time.

Workaround: Limit the number of source addresses available for NAT translation to less than 2000, or increase traffic slowly.

- CSCsx58335

Symptoms: When relaying to multiple servers from an unnumbered interface, the DHCP relay sends packets to all servers, even for packets where the client is in a RENEWING state unicasting to attempt to reach a single server. ARP entries are retained for all offered addresses, even if the client is ultimately using a different address. These extra ARP entries persist for several hours.

Conditions: The symptom is observed under the following conditions:

1. When relaying a DHCP packet on an unnumbered interface and the DHCP client is in a renewing state (as determined by the fact that the packets are sent to the DHCP server that allocated the address so that we do not end up giving the client a new address, which would then interrupt the user sessions).
2. When the client is in any other state, or if we do not get a response from the DHCP server, the packets are sent to all helper-addresses.

Workaround: Use Cisco IOS Release 12.4T images.

Further Problem Description: Retain only an ARP entry for the address that the DHCP client acknowledges. Do not retain addresses offered by DHCP servers that the client did not use in the ARP table.

- 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. More than one 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 that are 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.

- CSCtb60330

Symptoms: SVTI tunnel flaps at phase 1 expiry when a DPD ACK is not received. The line protocol on the tunnel interface goes down.

Conditions: This symptom is observed with SVTI tunnels and when DPDs are enabled.

Workaround: Disable DPDs.

Alternate Workaround: Use the **no crypto isakmp keepalive** command.

Further Problem Description: This symptom may affect those scenarios where routing protocols like BGP are run over the tunnel. To diagnose this problem, the following debugs should be enabled on both sides:

- **debug crypto isakmp**
- **debug crypto ipsec**
- **debug crypto kmi**

The following entry can be seen in the debugs:

```
DPD sent to 10.1.1.1:500 & waiting: But IKE sa expired. Killing IPSec sas.
```

- 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.

- 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 <hostname> 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 and then configuring it again. Commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

Workaround: There is no workaround.

- CSCtd75033

Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.



Note The fix for this vulnerability has a behavior change effect on Cisco IOS Operations for Mode 7 packets. See the section “Further Description” of this release note enclosure.

Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

This is the same as the vulnerability which is described in <http://www.kb.cert.org/vuls/id/568372>.

Cisco has released a public facing vulnerability alert at the following link:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=19540>

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router# show running-config | include ntp
```

```
ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
router# show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example shows a product that is running Cisco IOS Software Release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in “White Paper: Cisco IOS and NX-OS Software Reference Guide” at the following link:

<http://www.cisco.com/web/about/security/intelligence/ios-ref.html>

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.



Note

NTP peer authentication is not a workaround and is still a vulnerable configuration.

* NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access

access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration
```



```
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled “Performing Basic System Management” at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

* Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

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 ACLs (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 below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well. The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the multicast group must
!---   be filtered as well. The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!---   to infrastructure addresses.

access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- 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 fastEthernet 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 and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, while the second looks at rate limiting NTP traffic to the box.

- Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP 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 can be configured on a device to help 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, which will help protect all devices with IP addresses in the infrastructure IP address range.

```

!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 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-udp-class
 match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
 class drop-udp-class

```

```

drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
service-policy input drop-udp-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.

- Rate Limiting the traffic to the device.

The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded, valid NTP traffic may also be dropped.

```

!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
class rate-udp-class
police 10000 1500 1500 conform-action transmit
exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
service-policy input drop-udp-traffic

```

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 and
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

- CSCte69555

Autonomous Access Point configured as Wireless Group Bridge with EAP-TLS authentication improperly validates certificates when acting as supplicant.

Conditions: Autonomous IOS previous to 12.4(21a)JY are affected but only if:

- AP is configured with the Workgroup Bridge (WGB) feature.
- WGB feature is configured to use EAP-TLS authentication.

This issue affects the AP only when it acts as a supplicant to join the network that it will bridge packets.

Workaround: There is no workaround.

Further Problem Description: If the autonomous access point is using WGB with EAP-TLS authentication configure the command “clock save interval 8” and have the access point synchronized via NTP or SNTP *before* upgrading to 12.4(21a)JY or later.

Failure to follow this requirements on WGP with EAP-TLS authentication autonomous access points might render the AP non-operational and reconfiguration from the console port.

Failure to follow this requirement on an autonomous access point that uses EAP-TLS to authenticate to the network might render the AP non-operational and require reconfiguration from the console port.

“clock save interval” and NTP are required to properly deploy WGB with EAP-TLS on autonomous access points without a hardware clock.

After the clock time has been learned through NTP or SNTP, the “clock save interval” command causes the date and time to be saved to NVRAM at the interval indicated by the command and during any shutdown process. The saved date and time will then be available the next time the access point reloads.

- 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.

- CSCtf13014

Symptoms: A DNS server on a router does not immediately serve its own primary zone, if next-layer DNS servers are configured (every query is forwarded to these servers first).

Conditions: The symptom is observed when next-level (parent) DNS servers are configured on the router.

Workaround: There is no workaround.

- 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.

- CSCtf91428

Symptoms: Router crashes in IP Input.

Conditions: NAT must be configured.

The customer who reported the crash was using bit torrent when it crashed.

The public interface was an ATM [DSL].

Workaround: There are no viable workarounds.

- CSCtg27206

Symptoms: A static route is not seen in the receiver end after a link flap.

Conditions: This symptom is observed if the reachability of the same subnet to static routes nexthop is being learned from another interface during link down, and, before link flap, RIP protocol is removed and reconfigured.

Workaround: Do a **clear ip route** *ip-address* on the sender side.

- CSCtg41733

Symptoms: Certain crafted packets may cause a memory leak on a Cisco IOS router.

Conditions: This symptom is observed on a Cisco IOS router that is configured for SIP processing.

Workaround: Disable SIP if it is not needed.

Resolved Caveats—Cisco IOS Release 12.4(25c)

Cisco IOS Release 12.4(25c) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25c) but may be open in previous Cisco IOS releases.

- CSCsc62963

Symptoms: The interface MTU is not user configurable. When you attempt to configure the **interface level command mtu** command, 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.

- CSCsg76408

Symptoms: Multicast traffic from a DMVPN spoke is dropped by a hub when CEF is enabled on the tunnel interface of the hub. This situation causes the spoke to remain in registering mode and the hub to forward the decapsulated data.

Conditions: This symptom is observed on a Cisco router in a DMVPN environment when the mGRE tunnel interfaces are within a VRF.

Workaround: Disable CEF on the tunnel interface of the hub. Doing so enables the hub to receive the multicast traffic, although the traffic is then process-switched.

- CSCsi46897

Symptoms: PPP may crash when an **snmpwalk** command is executed on the cbQosSetStatsTable object.

Conditions: This symptom is observed when a service policy with a child policy that contains marking ("set") actions is applied to an interface before the **snmpwalk** command is executed on the cbQosSetStatsTable object of the CISCO-CLASS-BASED-QOS-MIB.

Workaround: There is no workaround.

- CSCsj01961

Symptoms: A router may not boot and may generate an “INSUFFICIENT MEMORY” error message.

Conditions: This symptom is observed on a Cisco 7600 series router that has an RSP720 when the ifIndex table is corrupt, preventing SNMP from initializing because SNMP attempts to use the ifIndex table from NVRAM.

Workaround: There is no workaround.

- CSCsj46859

Symptoms: Real Time Streaming Protocol (RTSP) inspection does not work with fragmentation.

Conditions: This symptom occurs only when fragmentation is set. Without fragmentation, this problem does not occur.

Workaround: There is no workaround.

- CSCsj47356

Symptoms: Phone A believes that its offer (in the first INVITE) is not answered yet, but this is wrong because UPDATE is for second leg where SDP answer is already sent in a 183 Session Progress.

Conditions: This symptom occurs in a call-forwarding scenario. A call comes in from PSTN to a SIP and is forwarded to a another SIP phone.

Workaround: There is no workaround.

- CSCsm44620

Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from two PEs (rpm-xf.13 and rpm-xf.11). After RP migration from AVICI to CRS, we found that tunnels from PE in slot 13 were not coming up. The PE in slot 13 was inconsistently in registering mode. The PE was not coming out of registering mode, which was preventing the tunnels from coming up. For the PE to come out of registering mode, S,G state should be built from new RP down to PE. At this stage, the CRS (RP) showed that the S,G tree was established at the RP. The S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to the PE, showed that the S,G state was established and that the PE-facing interface was in OIL. But there were a couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of the PE. In addition, we found that the PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for the PE to remain in registering mode, hence preventing the tunnels from coming up.

Workaround: Remove the following configurations:

- a. rpm-xfh10-z135—Shut and remove interface Switch1.4073.
- b. rpm-xfh09-z134—Shut and remove interface Switch1.4073.
- c. rpm-xfp11-1172—Remove interface Switch1.3172.
- d. rpm-xfp13-z074—Remove interface Switch1.4074.
- e. rpm-xfp04-1171—Remove interface Switch1.3171.

- CSCsm46114

Symptoms: Applications that require ALG processing (FTP, DNS, H.323) do not go through NAT NVI.

Conditions:

- NAT NVI is configured on one PE to provide access to Internet via packet-leaking configuration.
- Traffic is initiated from CE connected to another PE.
- Traffic reaches PE/NAT through the VPN across MPLS cloud.

Topology is as follows: CE---PE---MPLS---PE/NAT---Internet

Workaround: There is no workaround.

Further Problem Description: This impacts all process-switched packets (not only packets that require ALG processing).

- CSCsm75286

Symptoms: A route map that is configured for a BGP peer does not work as expected. The issue is not specific to BGP; it could also happen with other protocols.

Conditions: This symptom is observed after the route map is modified to delete a sequence.

Workaround: Apply a fresh route map.

- CSCsq58289

Symptoms: The connected interface prefix that is redistributed to OSPF is not seen as a Type 5 LSA in the OSPF database.

Conditions: The symptom is observed with the prefix that is initially covered by a “network ...” statement under **router ospf ...** and later removed by doing **no router ospf ...** instead of **no network**

Workaround: Perform a **shut** then **no shut** on the interface with the prefix that is not being redistributed.

- CSCsq99299

Symptoms: A router crashes during traceback generation with a bus error.

Conditions: When a CPUHOG occurs, a traceback is generated. In some cases, this may lead to a crash because of uninitialized internal data.

Workaround: There is no workaround.

- CSCsu71818

Symptoms: A Cisco 7206VXR (NPE-G1) experiences memory corruption and then crashes.

Conditions: This symptom occurs on a Cisco 7206VXR (NPE-G1) that is very busy running NAT.

Workaround: There is no workaround.

- CSCsu96698

Symptoms: More specific routes are advertised and withdrawn later even if the **config aggregate-address net mask summary-only** command is configured. The BGP table shows the specific prefixes as suppressed with s>.

Conditions: This symptom occurs only with very large configurations.

Workaround: Configure a distribute list in the BGP process that denies all of the aggregation child routes.

- CSCsv92961
Symptoms/Conditions: Traffic does not resume when the interface between the PE and the receiver CE is bounced.
Workaround: There is no workaround.
- CSCsw84994
Symptoms: A Cisco 7301 router may experience a lot of CPU hogs due to the SSGTimeout process:

```
%SYS-3-CPUHOG: Task is running for (2008)msecs, more than (2000)msecs  
(116/59),process = SSGTimeout.
```


Conditions: The symptom is observed on a Cisco 7301 router.
Workaround: There is no workaround.
- CSCsx32283
Symptoms: A router crashes.
Conditions: This symptom occurs because of malformed LDAP packets.
Workaround: There is no workaround.
- CSCsx68596
Symptoms: The system may display a %SYS-3-NOELEMENT message similar to the following:

```
%SYS-3-NOELEMENT: data_enqueue:Ran out of buffer elements for enqueue -Process=  
"<interrupt level>", ipl= 6
```


After which the system behavior can be unpredictable. If the interrupts are rapid enough, the system may become unresponsive (hang), use all available memory to create more buffer elements, or crash due to CSCsj60426.
Conditions: The message is caused by extremely rapid changes in flow control or modem control lead status on a console port.
Workaround: Eliminate the source of the rapid lead changes. As modem control and flow control are generally not supported on the console, these changes are usually due to misconfigured devices that are attached to the console.
- 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.
Workaround: There is no workaround.
- CSCsy24642
Symptoms: A router that is running Cisco IOS software may leak memory.
Conditions: This symptom may be observed when a QoS policy is used on a low-speed multilink interface. If the interface does not have enough bandwidth to support the policy, some memory will leak.
Workaround: Suppress QoS.
- CSCsy29533
Symptoms: A T.38 fax-relay call may fail.
Conditions: This symptom is observed with an MGCP-controlled T.38 fax-relay call when the gateway is configured for CA control T.38. The output of the **debug voip vtsp all** command shows fax relay as "DISABLED."
Workaround: Use Cisco IOS Release 12.4(15)T7 or Release 12.4(22)T.

- CSCsz45419

Symptoms: The WORD option is not displayed in some of the NTPv4 commands. Some NTP commands are not working properly.

Conditions: This symptom occurs on a Cisco router that is running an internal build of Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCsz50423

Symptoms: The **clear interface atm5/ima** command makes the ATM PVC inactive.

Conditions: This symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 12.4(24.6)T8.

Workaround: There is no workaround.

- CSCsz62850

Symptoms: Intermittent failure of VRF-aware NAT. After an outside-to-inside translation, the packet is routed based on the global routing table instead of the VRF routing table. This symptom is observed in only 1 to 2 percent of traffic.

Conditions: This symptom occurs in Cisco IOS Release 12.4(23). It may not occur in Cisco IOS Release 12.4(10), but this is not yet confirmed.

Workaround: There is no workaround.

- CSCsz70666

Symptoms: The **show version** command shows the reload reason as “power-on.”

Conditions: This symptom occurs on a Cisco AS5850 that is configured for HOS mode when it is rebooted with a time lag.

Workaround: There is no workaround.

- 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 **dlsw local-peer** command automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw 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:

dlsw remote-peer 0 fst ip-address

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 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:

dlsw 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 customers environment.

- CSCsz71831

Symptoms: An interface may hold several DNS packets in the interface buffers and not be released until an upgrade of the device.

Conditions: This symptom has been observed only on low-end router systems, which are configured to listen on TCP/UDP port 53 (DNS).

Affected configurations would include any configuration that has either:

```
ip dns server
ip dns spoofing
ip dns primary
```

And can be verified the device is listening via the **show udp**, **show ip socket**, or **show tcp brief all** command.

It is not possible to wedge the entire interface, to cause a DoS, but around half the interface buffers may be consumed.

Workaround: The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

* Disable Affected Listening Ports If the DNS feature is not required it can be explicitly disabled. Once disabled confirm the listening UDP port has been closed by entering the CLI command **show udp** or **show ip socket**. Some features may require a reload of the device after disabling the feature in order to close the listening UDP port.

* Infrastructure Access Control Lists

Warning: Because the DNS feature in this vulnerability utilize UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

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 this specific vulnerability. 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: Domain Name Service (DNS)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 53

access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 53

!--- Deny DNS traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
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 and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Control Plane Policing

Warning: Because the DNS feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP 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 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 which will protect all devices with IP addresses in the infrastructure IP address range.

```
!---
```

```
!--- Feature: Domain Name Service (DNS)
```

```
!---
```

```
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 53
```

```
access-list 150 deny tcp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 53
```

```
!---
```

```
!--- Deny DNS traffic from all other sources destined
```

```
!--- to the device control plane.
```

```
!---
```

```
access-list 150 permit udp any any eq 53
```

```
access-list 150 permit tcp any any eq 53
```

```
!---
```

```
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
```

```
!--- Layer4 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-dns-class match access-group 150
```

```
!---
```

```
!--- Create a Policy-Map that will be applied to the
```

```
!--- Control-Plane of the device.
```

```
!---
```

```
policy-map drop-dns-traffic class drop-dns-class drop
```

```
!---
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
!---
```

```
control-plane service-policy input drop-dns-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-dns-traffic class drop-dns-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/gtrtlmt.html

Exploit Detection: It is possible to detect blocked interface queues with an Cisco IOS Embedded Event Manager (EEM) policy. EEM provides event detection and reaction capabilities on a Cisco IOS device. EEM can alert administrators of blocked interfaces with e-mail, a syslog message, or a Simple Network Management Protocol (SNMP) trap.

A sample EEM policy that uses syslog to alert administrators of blocked interfaces is available at Cisco Beyond, an online community dedicated to EEM. A sample script is available at the following link:

<http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=981>

Further information about EEM is available from Cisco.com at the following link:

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

- CSCsz72591

Symptoms: A router crashes with an Address Error (load or instruction fetch) exception.

Conditions: The router must be configured to act as a DHCP client.

Workaround: There is no workaround.

- CSCsz72701

Symptoms: DSP crashes are recorded.

Conditions: This symptom is observed with a large volume of calls.

Workaround: Reboot.

Further Problem Description: The crash dump files indicate that some large packets are sent to DSP.

- 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.

- CSCta39763

Symptoms: A Cisco router may experience a memory leak in the “ISDN Call Tabl” process, as seen in the output below:

```
Router# show memory all totals
```

```
Allocator PC Summary for: Processor Displayed first 2048 Allocator PCs only
PC Total Count Name 0x6010B9E8 9891336 513 ISDN Call Tabl
```

Conditions: This symptom has been experienced on a Cisco 3845 router that is running Cisco IOS Release 12.4(22)T with ISDN configured.

Workaround: There is no workaround.

- 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.

- 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 re-enabling MGCP with version 1.0 after testing fgdn calls with MGCP version 0.1.

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.

- CSCta77678

Symptoms: The RTP timestamp on the RFC-2833 event is modified. IP Phones are using RFC 2833 to transport the DTMF signals, which causes problems with the voice-mail 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.

- CSCta85026

Symptoms: The CLI does not accept white spaces in the DHCP option 60 Vendor Class Identifier (VCI) ASCII string and displays the following error message:

```
Router(dhcp-config)# option 60 ascii Cisco AP c1240
% Invalid input detected at '^' marker.
Router(dhcp-config)#
```

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T1 and later releases.

Workaround: There is no workaround.

- CSCta87146

Symptoms: There are no flows in the NetFlow cache when PFR is enabled.

Conditions: The symptom is observed when PFR is enabled.

Workaround: Disable PFR.

- CSCtb16459

Symptoms: Unable to export traffic from interfaces (other than Ethernet) using RITE.

Conditions: This symptom occurs when trying to configure “interface integrated-service-engine 1/0” under “ip traffic-export profile test.”

Workaround: There is no workaround.

- CSCtb17856

Symptoms: H.323 calls may intermittently fail with cause code 41. Depending on traffic, after several days, calls may start failing with cause code 47.

Conditions: This symptom may occur when there is a race condition in setting up an H.245 session between H.323 peers and we end up with two separate H.245 sessions simultaneously.

Workaround: There is no workaround for cause code 41. But if you start getting too many cause code 47, reloading will help alleviate symptoms for some time.

- CSCtb17881

Symptoms: A router crashes when an HQoS service policy is removed and added back to a fr-subinterface while traffic is flowing.

Conditions: The crash happens when the following configuration is applied to the fr-subinterfaces:

- fr payload compression
- HQoS policy with WRED in child policy

With this configuration and traffic flowing through the interface, if the QoS policy is removed and added back to the fr-subinterface, there is a chance that the router will crash.

Workaround: There are a few workarounds:

- Do not have fr payload compression and an HQoS service policy on the fr-subinterface at the same time.
- Remove the WRED configuration from the HQoS policy.

- CSCtb23504

Symptoms: When Cisco IOS IKE DPD is enabled, the rekey does not happen.

Conditions: This symptom occurs when IKE DPD is enabled.

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.

For more information on restricting traffic to VTYS, please consult:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

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.

- CSCtb66295

Symptoms: There is no IP connectivity because of an erroneous ARP table.

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 12.4(24)T, 12.4(24)T1, and 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_paper09186a00801a1a55.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/gtrtlmt.html

- CSCtb71569

Symptoms: Packet drops happen on LLQ before crypto when a service policy that uses Hierarchical Shaping is applied to a tunnel interface and crypto hardware is used.

Conditions: Cisco 7200VXR + Crypto hardware (VPN acceleration Module) 12.3(22.7) or later. 12.4(12.15b) or later. 12.4(13.5)T or later.

Workaround: There is no workaround.

- CSCtb72550

Symptom: CDR records are pushed via FTP to a file fail with any Cisco IOS release that contains the fix for CSCta23301.

Conditions: This symptom is observed when “gw-accounting file” is configured to point to an FTP server and the fix for CSCta23301 is present.

Workaround: Downgrade to a version of Cisco IOS software that does not contain the fix for CSCta23301 or push the CDR records locally to flash instead of to an FTP URL.

- 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.
- The **no ccm-manager** command is entered.

Workaround: Do not shut down the voice port at the time of configuration download.

- 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.

- CSCtb93424

Symptoms: A Catalyst 6K CMM (Cisco Communications Module) with a media card that is running Cisco IOS Release 12.4(15)T3 might crash upon issuing the **show mediacard dsp channel** command.

Conditions: The DSPs on the media card must be registered to a Cisco Unified CallManager and must be configured to act as a transcoding resource.

Workaround: There is no workaround.

- CSCtb95275

Symptoms: Autocommands configured on a VTY line or user profile are not executing while logging through VTY.

Conditions: This symptom is observed if the privilege level is not configured in the user profile.

Workaround: Explicitly configure the user privilege level in the user profile.

- CSCtc04228

Symptoms: The **mgcp behavior g729-variants static-pt** command 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 enabled previously.

Conditions: Using an earlier version of a Cisco IOS release will enable the command.

Workaround: After downgrading to a lower version where the **mgcp behavior g729-variants static-pt** command is not the default, configure the **no mgcp behavior g729-variants static-pt** command to remove the CLI.

- CSCtc11521

Symptoms: An 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 back up 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.

- 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.

- CSCtc19036

Symptoms: A traceback from function `k_rttMonEchoAdminEntry_ready` is displayed while an SNMP operation is being performed.

Conditions: This symptom is observed when using SNMP to create an IP SLA jitter probe that includes a codec option.

Workaround: There is no workaround.

- CSCtc32374

Symptoms: ISDN Layer 1 is deactivated after a reload, and calls fail with cause code 47 (Resource Unavailable).

Conditions: This symptom is observed when the **busyout monitor** command 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 the Layer 2 to a MULTIFRAME-ESTABLISHED connection status, but calls still fail with cause code 47.

- CSCtc55734

Symptoms: A Cisco IOS router crashes at boot-time with a Breakpoint exception error:

```
program load complete, entry point: 0x80010000, size: 0x11cdd28 Self decompressing
the image :
#####
##### [OK]
System received a divide by zero exception
: Breakpoint exception, CPU signal 8, PC = 0x61530874

----- Possible
software fault. Upon recurrence, please collect crashinfo, "show tech" and contact
Cisco Technical Support.
-----

-Traceback= $0 : 00000000, AT : 62330000, v0 : 00000001, v1 : 00000000 a0 : 00000000,
a1 : 00000000, a2 : 00000000, a3 : 00000000 t0 : 00000000, t1 : 00000000, t2 :
00000000, t3 : 6232C6A4 t4 : 00000000, t5 : 62470000, t6 : 00000000, t7 : FEED0000 s0
: 00000000, s1 : 00000000, s2 : 62660000, s3 : 27BD0000 s4 : 60010000, s5 : 60010000,
s6 : 62170000, s7 : 0020002F t8 : 00000001, t9 : 00000077, k0 : 30408001, k1 : B0020000
gp : 62334450, sp : 8000FD90, s8 : 68000001, ra : 613BFD44 EPC : 61530874, ErrorEPC
: BFD85CFC, SREG : 34008003 MDLO : FFFFFFFF, MDHI : 00000001, BadVaddr : 7ADCBEFD
DATA_START : 0x61543050 Cause 00000024 (Code 0x9): Breakpoint exception
```

Conditions: This behavior is observed on any Cisco IOS router that is installed with Cisco IOS Release 12.4(25b)M0.6. All feature sets are affected.

Workaround: Use Cisco IOS Release 12.4(25b)M0.5 or an earlier release in the Cisco IOS 12.4 mainline release family.

- CSCtc58898

Symptoms: In an MPLS VPN scenario, if it happens that the default route known via RIP in the VRF is looping, the route might stay in the RIB.

Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SRC4 and 12.2(33)SRC5.

Workaround: Clear the VRF routing table using the **clear ip route vrf name *** command.

- CSCtd25213

Symptoms: NAT is not working for locally generated packets.

Conditions: This condition is observed when NAT is configured for inside and outside addresses and when a self-generated packet is sent to OL.

Workaround: Instead of using dynamic NAT, use static NAT for self-generated packets.

- CSCtd98344

Symptoms: NAT/PAT does not create more than one translation entry for all VRFs after there is a translation in the first VRF.

Conditions: This symptom is observed when there is more than one VRF.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(25b)

Cisco IOS Release 12.4(25b) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25b) but may be open in previous Cisco IOS releases.

- CSCsk80250

Symptoms: A router may reload.

Conditions: This symptom is observed when the **show ip bgp neighbors x.x.x.x paths ^([⁷][⁰][¹][⁸]l.l.l.l.....)+_7018_** command is issued.

Workaround: There is no workaround.

- CSCsk86410

Symptoms: Abnormal ISAKMP traffic causes an alignment error and traceback on the device.

Conditions: This symptom is observed when a malformed IKE packet is sent to the router that is running an affected version of Cisco IOS software. The router functionality is not affected by this and continues to function normally.

The following is an example of an alignment traceback:

```
%ALIGN-3-TRACE: -Traceback= 0x437E53B0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

Workaround: There is no workaround.

- CSCsl15443

Symptoms: Console port can lock up after 10-15 minutes. Telnet sessions fail.

Conditions: Occurs when terminal server is connected to router's console port.

Workaround: There is no workaround.

- CSCso06542

Symptoms: On a Cisco router that is configured for NAT VPN routing/forwarding (VRF), **ip nat inside source** commands might get corrupted at bootup time in the running config even though they are perfectly fine in the startup config. The corruption can be observed in the following form (but not only):

```
ip nat inside source list [ACL] pool [pool-name] vrf [vrf-name] match-in-vrf overload
vrf [vrf-name]
```

The “**vrf** [*vrf-name*]” after **overload** should not be there.

Conditions: This symptom was observed on a Cisco 3845 running Cisco IOS Release 12.4(18.3)T and configured with NAT VRF, but it can be observed on other platforms and Cisco IOS versions.

Workaround: Remove and re-configure the affected VRFs. The problem might re-appear after bootup.

- CSCso52837

Symptoms: The following error is received:

```
%Error parsing filename (No such device)
```

Conditions: This symptom is observed when the **copy run disk0:test** command is executed.

Workaround: Use a “/” as in **copy run disk0:/test**.

- CSCsr60092

Symptoms: One-way audio is observed after use of TCL [connection create] command.

Conditions: Occurs with TCL application playing media in incoming_leg and leg setup without bridging incoming leg [leg setup \$dnis callInfo].

Workaround: There is no workaround.

- CSCsr96084

Symptoms: A router crashes with the following error:

```
%SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000
```

Conditions: The symptom is seen on routers that are running Dynamic Multipoint VPN (DMVPN) when a routing loop occurs while an NHRP resolution request is received by the router. If the routing loop leads to a tunnel recursion (where the route to the tunnel endpoint address points out of the tunnel itself) the crash may be seen.

Workaround: Use PBR for locally-generated traffic to force the GRE packet out of the physical interface, which prevents the lookup that can lead to the recursion. For example (note: the interfaces and IPs will need to be changed to the appropriate values):

```
interface Tunnel97
...
tunnel source POS6/0
...

interface POS6/0
ip address 10.2.0.1 255.255.255.252
ip local policy route-map Force-GRE
ip access-list extended Force-GRE
permit gre host 10.2.0.1 any

route-map Force-GRE permit 10
match ip address Force-GRE
set interface POS6/0
```

- CSCsv40924

Symptoms: A Cisco router that is running NAT may corrupt the IP header checksum for some RTSP packets.

Conditions: This symptom is observed when the RTSP connection goes through NAT, “OPTION” or “DESCRIBE” messages are sent, and the NAT translation used has a differing number of characters for the private and public IP addresses of the server.

Workaround:

- 1) Configure the **no-payload** command for the NAT translation. This will stop the corruption, but will also cause all deep packet NATing to stop, which can cause other issues.
- 2) Use a port other than 554 for the RTSP stream. This will stop the corruption, but will also stop the router from NATing the embedded IP addresses in the RTSP packets. Depending on the specific implementation of RTSP, this may or may not stop the stream from working.
- 3) Change your NAT translation such that the private and public IP addresses have the same number of characters. For instance 192.168.0.1 has 11 characters, and 172.16.100.200 has 14 characters.

- CSCsw23664

Symptoms: Reverse Route Injection (RRI) is not working as expected with VPN routing/forwarding (VRF) aware IPsec. Routes are created but may not be removed, leaving them stranded in the routing tables.

Conditions: This symptom occurs on routers that are running Cisco IOS Release 12.4 Mainline.

Workaround: There is no workaround.

- CSCsw40203

Symptoms: A Cisco ASR 1000 may crash with certain malformed IKE packets.

Conditions: This symptom is observed on a Cisco ASR 1000 that is configured for IPsec VPN with digital certificates.

Workaround: There is no workaround.

- CSCsw98414

Symptoms: The **ip nat inside source ... match-in-vrf** command is not working without the **overload** option.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(15)T8 or another affected release.

Workaround: There is no workaround.

- CSCsx03120

Symptoms: When an ATM interface on a WIC1-ADSL comes back up after a flap, under some undefined circumstances, it may be observed that none of the configured PVCs forward traffic.

Conditions: Specific conditions are still under investigation.

Workaround: Perform a **shut/no shut** on the interface or power-cycle the router.

- CSCsx20984

Symptoms: A router reloads with a bus error and no tracebacks.

Conditions: Unknown at this time.

Workaround: There is no workaround.

- CSCsx33622

Symptoms: Flapping BGP sessions are seen in the network when a Cisco IOS application sends full-length segments along with TCP options.

Conditions: This issue is seen only in topologies where a Cisco IOS device is communicating with a non-Cisco-IOS peer or with a Cisco IOS device on which this defect has been fixed. The router with the fixed Cisco IOS software must advertise a lower maximum segment size (MSS) than the

non-fixed Cisco IOS device. ICMP unreachable toward the non-fixed Cisco IOS router must be turned off, and TCP options (for example, MD5 authentication) and the **ip tcp path-mtu-discovery** command must be turned on.

Workaround: Any value lower than the advertised MSS from the peer should always work.

Setting the MSS to a slightly lower value (-20 to -40) is sufficient to avoid the issue. This number actually accounts for the length of TCP options present in each segment. The maximum length of TCP option bytes is 40.

If the customer is using MD5, Timestamp, and SACK, the current MSS should be decreased by 40 bytes. However, if the customer is using only MD5, the current MSS should be decreased by 20 bytes. This should be enough to avoid the problem. For example:

1. If the current MSS of the session is 1460, New MSS = 1460 - 40 = 1420 (accounts for maximum TCP option bytes; recommended).
 2. If the current MSS of the session is 1460, New MSS = 1460 - 20 = 1440 (accounts for only the MD5 option).
- CSCsx34297

Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-IOC3/PA-POS-2OC3.

Conditions: The symptom is observed on a Cisco 7200 series router and Cisco 7301 router with an NPEG1 processor.

Workaround: Change the MDL of operation to PULL using the **dma enable pull model** command.

- CSCsx49573

Symptoms: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

The Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml>

Conditions: See the “Additional Information” section in the posted response for further details.

Workarounds: See the “Workaround” section in the posted response for further details.

- CSCsx67255

Symptoms: An outgoing call from an IP phone to PSTN through ISDN PRI fails on a channel due to a DSP allocation failure (not enough DSPs to support the call). Subsequent calls through that same channel continue to fail with “resource unavailable” cause value equal to 47 even after DSP resources have been made available to handle the call.

Conditions: The symptom occurs on a router running Cisco IOS Release 12.4(15)T8 or higher. The call must first fail with a legitimate DSP allocation error. Any call made through the same channel as the failed call will also fail.

DSP allocation failures on gateway can be checked through the use of the exec command **show voice dsp group all**. The last line of the show command output includes a counter for “DSP resource allocation failure.”

This issue can be seen also in some cases upon bootup. When a gateway is reloaded, system resources will come up with slightly different timing. If, for example, a PRI interface comes up before the DSP resources have fully initialized, there may be a similar failure.

Workaround:

1. Reload the router to clear the channel. If a reload cannot be done, busy out the channel with the failed calls using the **isdn busy b_channel** command under the serial interface.

2. If this issue is due to oversubscription of the DSP resources, change the configuration to meet the DSP resources available on the gateway. Further information can be found with the CCO “DSP Calculator” at http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl.
 3. If the issue is related to timing issues upon reload, shutdown the voice-port in question before reloading the gateway. When the gateway comes back up, take the voice-port out of shutdown.
- CSCsx75353

Symptoms: High CPU usage is observed on a Cisco 2821 router. An increase of almost 10 percent in CPU utilization is observed with every voice call.

Conditions: This symptom is observed when an AIM compression card is present on the motherboard (specifically AIM-COMPR2-V2).

Workaround: Remove the AIM compression card from the motherboard.
 - CSCsy10653

Symptoms: Calls on an MGCP gateway negotiating the g729br8 codec may fail to have audio in one or both directions.

Conditions: This occurs on MGCP gateways with the fix for CSCsu66759 when the g729br8 codec is being negotiated.

Workaround: Any of the following will be sufficient to get around this issue:

 1. Configure the gateway for static payload type using the following commands on the gateway:


```
mgcp behavior g729-variants static-pt
mgcp behavior dynamically-change-codec-pt disable
```
 2. Disable g729br8 from being negotiated for this call. If CUCM is involved, this is done with the service parameter “Strip G.729 Annex B (Silence Suppression) from Capabilities.”
 3. Use a Cisco IOS code on the gateway which does not contain the fix for CSCsu66759 (Cisco IOS Release 12.4(22)T and below).
 - CSCsy16092

Symptoms: A router that is running Cisco IOS or Cisco IOS XE may unexpectedly reload due to a watchdog timeout when there is a negotiation problem between crypto peers. The following error will appear repeatedly in the log leading up to the crash:

```
.Mar 1 02:59:58.119: ISAKMP: encryption... What? 0?
```

Conditions: When a malformed payload (Transform payload with vpi length =0) is received and the **debug crypto isakmp** command is enabled, the error messages are repeatedly seen leading up to the crash.

Workaround: Remove this **debug** command.
 - CSCsy32768

Symptoms: Layer 2 tunneled traffic stops working when PIM is configured.

Conditions: This symptom is observed when following conditions are met:

 - The device is a Cisco 7200 and is running any Cisco IOS 12.4 mainline version.
 - The NPE port is used with multiple subinterfaces.
 - PIM and L2TPv3 are configured on different subinterfaces on the main NPE interface.

Workaround: This issue is not seen in 12.4T. You can switch to the T train; there are no known workarounds at this point.

- CSCsy60426

Symptoms: High CPU utilization occurs when editing the ACL entries on a router running the c7301-ik9s-mz.124-23 image. The problem does not exist in the c7301-ik9s-mz.123-23 image.

Conditions: Occurs when two Cisco 7301 routers are configured for VPN redundancy. The **crypto dynamic-map** command is configured with match address to match crypto ACL that has 215 ACL entries. There are 1300 IPsec tunnels. The active router is running 7301-ik9s-mz.124-23, and the standby router is running c7301-ik9s-mz.123-23.

The HIGH CPU problem is reported only on the router that is running 7301-ik9s-mz.124-23:

CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 95%

```
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
148 1085948 1402983 774 98.49% 97.28% 93.63% 0 Crypto IKMP
149 44592 86808 513 0.00% 0.00% 0.00% 0 IPSEC keyengine
```

The following steps reveal the problem:

- There is a named ACL configured in the VPN router which defines the interesting traffic criteria for the establishment of the IPsec tunnel.
- Enter configuration mode and add or remove entries from the named ACL.
- Exit configuration mode. CPU utilization goes up to 99% momentarily on the router running Cisco IOS Release 12.3. After 4 seconds it returns to normal. On the router running Cisco IOS Release 12.4, CPU utilization stays high and affects router operations.

Workaround: Shift the tunnels over to the standby VPN by lowering the HSRP priority manually in the problematic router.

- CSCsy87674

Symptoms: Calls via an MGCP gateway that is registered to a Cisco Unified Communications Manager (CUCM) fail immediately with a codec negotiation error.

Conditions: This symptom is observed when a CUCM is configured to use the G729 codec for the MGCP gateway.

Workaround: Use the G729 AnnexB codec between the MGCP gateway and the CUCM.

- CSCsz08955

Symptoms: This is a rarely occurring crash when ssg portmap and Transparent Auto Logon (TAL) are enabled together on a PPP session.

Conditions: There is a timing issue that leads to a crash when ssg portmap and TAL are enabled together and when the PPP connection is terminated at the same time.

Workaround: There is no workaround when both features are present in the configuration. It can be avoided when only one feature is present.

Further Problem Description: When a session is being re-authenticated because of TAL and the PPP session is terminated at that time and also if it so happens that the connection has been idle for a while, then, because of timing issues in data structures, a situation might arise that can lead to a router crash.

The solution will be available in the next release.

- CSCsz29815

Symptoms: TTY sessions not accessible after reverse SSH session to the same TTY port results in failed authentication.

Conditions: Occurred on a router running Cisco IOS Release 12.4(24)T and configured with TTY lines accessed using reverse SSH Version 2. Issue also affects SSH version 1 and affects VTY lines.

Workaround: Reload the router.

- CSCsz55055

Symptoms: Attaching or removing a service policy flaps the Gigabit Ethernet interface.

Conditions: This symptom is observed only with a Cisco 3845 NM-1GE.

Workaround: There is no workaround.

- CSCsz56169

Symptoms: A software-forced crash occurs after a **show user** command is performed.

Conditions: The crash occurs after the user performs a **show user** command and then presses the key for next page. It is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(21a).

Workaround: Do not perform a **show user** command.

- CSCsz87499

Symptoms: Memory leaks occur for SIP calls in a SIP gateway.

Conditions: Occurs with regular SIP calls from PSTN through SIP voice gateway.

Workaround: There is no workaround.

- CSCsz87529

Symptoms: Gateway crashes due to lack of memory.

Conditions: Memory leak occurs in RTCP while processing calls. Due to lack of memory, the gateway crashes.

Workaround: There is no workaround.

- CSCta04391

Symptoms: A router with dynamic NAT for unicast and multicast traffic crashes after **ip nat inside source list** is deleted.

Conditions: Router crashes when there is unicast and multicast traffic and only when unicast and multicast traffic uses the same NAT rule.

Workaround: Use separate NAT rule for unicast and multicast traffic.

- CSCta77552

Symptoms: A Cisco 5850 crashed 2 minutes after the card in slot 5 crashed.

Conditions: This symptom was observed on a Cisco 5850 with Cisco IOS Release 12.4(25).

Workaround: There is no workaround.

- CSCtb07338

Symptoms: A traceback may occur.

Conditions: This symptom is observed after a crypto map is removed and reapplied.

Workaround: Use software encryption.

- CSCtb12334

Symptom: A traceback is seen when SNAT is unconfigured from the active router.

Conditions: This symptom is observed on Cisco routers that are running a Cisco IOS Release 12.4(25)M0.3 image.

Workaround: There is no workaround.

- CSCtb13491

A malformed Internet Key Exchange (IKE) packet may cause a device running Cisco IOS Software to reload. Only Cisco 7200 Series and Cisco 7301 routers running Cisco IOS software with a VPN Acceleration Module 2+ (VAM2+) installed are affected. Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100324-ipsec.shtml>.

Resolved Caveats—Cisco IOS Release 12.4(25a)

Cisco IOS Release 12.4(25a) is a rebuild release for Cisco IOS Release 12.4(25). The caveats in this section are resolved in Cisco IOS Release 12.4(25a) but may be open in previous Cisco IOS releases.

- CSCek77849

Symptoms: BGP convergence is very slow, and CPU utilization at BGP router process can reach 100% during the convergence at aggregation router. During normal operation, if BGP prefixes included in the aggregation flap, it will also produce high CPU utilization.

This issue shows the following tendencies:

1) The more of the component prefixes belonging to the aggregate-address entry, the slower the convergence at aggregation router. 2) The more of the duplicated aggregation component prefixes for aggregate-address entry, the slower convergence at aggregation router.

Conditions: Any releases would be affected if “aggregate-address” is configured, and routing updates involving aggregate components are received every few seconds.

Workaround: Remove the “aggregate-address”.

- CSCsc30830

Symptoms: There is an intermittent crash with four “conferencing and transcoding” cards installed.

Conditions: This crash is due to an initialization problem in ms_ac_dsprn during bootup.

Workaround: Do not configure no sccp, sccp or lower the number of act “conferencing and transcoding” cards.

- CSCsg96436

Symptoms: EzVPN router might lose its IPSec connection due to three consecutive missed keepalives.

Conditions: Occurs when ISAKAMP keepalives are configured with EzVPN.

Workaround: Disable keepalives.

- CSCsi78783

Symptoms: Router crashes when **auto qos voip** is configured on ATM-PVCs. It does not crash when **auto qos voip trust** or **auto qos voip** are configured on any interface.

Conditions: Occurs when **auto qos voip** is configured the first time on any ATM-PVC.

Workaround: Configure **auto qos voip** on any interface, such as a serial interface, and then configure **auto qos voip** on the ATM-PVC. Use **auto qos voip trust** if it is suitable for the network.

Further Problem Description: If **auto qos** exists in the startup configuration then the issue is not seen. It is seen only when it is configured on a ATM interface of a router which is up and running.

- CSCsy15227

Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

- CSCsy56320

Symptoms: If a T1/E1 controller on NM-CEM-4TE1 CEM module is configured for **clock source internal** so that it gets its clocking reference from the TDM backplane of a Cisco 2800 or 3800 Integrated Services Router (ISR), and the CEM T1/E1 controller flaps DOWN and then UP, the NM-CEM-4TE1 may cease being synchronized to the TDM backplane. Measurement and comparison of the clocking between the TDM backplane and the CEM T1/E1 shows that timing slips are occurring.

Conditions: This behavior may be observed on a Cisco 2800 or 3800 ISR which has been installed with a NM-CEM-4TE1 CEM module, and is running a Cisco IOS release from the 12.4 mainline train. The CEM T1/E1 controller is set for **clock source internal**.

Workaround: Two workarounds are known:

1. Manually set **clock source line** and then **clock source internal** under the CEM T1/E1 controller. The CEM T1/E1 controller and the TDM backplane will be in synchronization from this point forward until the next T1/E1 flap.
2. (This behavior is not known to affect Cisco IOS Release 12.4T release. If Cisco IOS Release 12.4T can be deployed, use a current release of this train.

- CSCsz23951

Symptoms: NSAP address family cannot be configured.

```
router bgp 1 address-family nsap <---- cannot be configured
```

Conditions: This symptom occurs on initial configuration.

Workaround: There is no workaround.

- CSCsz32366

Symptoms: A Cisco router that is running Cisco IOS Release 12.4(25) may crash due to SSH.

Conditions: This symptom occurs when SSH is enabled on the router. An attempt to access the router via SSH is made.

Workaround: Do not use SSH. Disable SSH on the router by removing the RSA keys:

```
"crypto key zeroize rsa"
```

Further Problem Description: This issue has not been seen in Cisco IOS Release 12.4(23) and earlier releases. It also has not been seen in Cisco IOS Release 12.4T images.

- CSCsz41177

Symptoms: On a Cisco IOS router with IPSec configured, if the IP address on an interface where the crypto map is applied to changes, then the crypto map configuration will disappear from the interface.

Conditions: This problem only occurs when there is an address change on the crypto map interface.

Workaround: Manually re-apply the crypto map after the IP address change on the interface.

- CSCsz48392

Symptoms: Doing reverse SSH to a TTY line, which is busy, causes the terminal server to crash.

Conditions: This issue is encountered in a Cisco 3845 router that is running Cisco IOS Release 12.4(23).

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.4(25)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(25). All the caveats listed in this section are open in Cisco IOS Release 12.4(25). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz30008

Symptoms: On a Cisco router, BGP peers may still initially come back up, wait for the timeout, and then stay down.

Additionally, after the RP has experienced an out-of-memory event, other problems may be experienced. For example if a malloc failure occurs while processing a BGP update, then router may report that the update was malformed and send a BGP notification. BGP may stop processing and sending updates, or alternatively may just stop sending updates. BGP may produce spurious memory accesses or the router may unexpectedly reload due to BGP.

Conditions: Occurs when the RP lacks sufficient memory.

Workaround: There is no workaround.

- CSCej33698

Symptoms: A router that is running Cisco IOS software may mistakenly fail a CRC check on files in NVRAM.

Conditions: This symptom has been observed with large files, such as large startup configurations.

Workaround: There is no workaround.

- CSCsf96266

Symptoms: Unable to obtain low latency for priority traffic while LLQ is configured.

Conditions: This is happening while LLQ is configured with IPsec and IPsec-GRE tunnels.

Workaround: There is no workaround.

- CSCsl15443

Symptoms: Console port can lock up after 10-15 minutes. Telnet sessions fail.

Conditions: Occurs when terminal server is connected to router's console port.

Workaround: There is no workaround.

- CSCsu66197

Symptoms: Cyclic redundancy check (CRC) errors increment on Cisco 2800 router.

Conditions: Occurs during normal operation.

Workaround: There is no workaround.

- CSCsu92724

Symptoms: The following errors are logged:


```
Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNTER: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT:
INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNTER:
Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback=
0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:25:
%ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99
Sep 21 05:07:25: %SYS-2-QCOUNTER: Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl=
4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238
0x600B220C Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNTER: Bad dequeue 62D74734 count
-1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:28: %ISDN-4-ISDN_UNEXPECTED_EVENT:
INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNTER:
Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback=
0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:28:
%ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99
Sep 21 05:07:28: %SYS-2-QCOUNTER: Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl=
4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238
0x600B220C
```

Conditions: Occurs when ISDN is enabled.

Workaround: There is no workaround.

- CSCsv05154

Symptom: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

The Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml>

Conditions: See “Additional Information” section in the posted response for further details.

Workaround: See “Workaround” section in the posted response for further details.

- CSCsv23797

Symptoms: ASR Router goes down.

Conditions: Occurs when kron policy is configured and SCP is used.

Workaround: Use regular SCP.

- CSCsv31812

Symptoms: Version: disk2:c7200-adventerprise9-mz.124-22.T on KSs and GMs:

```
Oct 26 18:41:50: %GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group
DGVPN-ALPHA from address 10.32.178.56 to 239.192.1.190 with seq # 23 Oct 26 18:41:50:
%SYS-3-MGDTIMER: Uninitialized timer, set_exptime, timer = 20A64C70. -Process= "Crypto
IKMP", ipl= 0, pid= 201, -Traceback= 0x6147CC48 0x62E75F4C 0x6392E05C 0x6392E300
0x63B25A70 0x63B25AF8 0x639308FC 0x63855544 0x6392F794 0x638100F4 0x638144E4
```

Conditions: KS2, CE1, and m-gm are connected to PE1. s-gm is connected to PE2. PE1 and PE are in MPLS cloud.

Lower the priority of KS1 and change the primary KS role from KS1 to KS2 by entering the **clear crypto gdoi ks coop role** command in KS1. KS2 becomes the primary. Tracebacks are seen in the KS2.

Workaround: There is no workaround.

- CSCsv40924

Symptoms: A Cisco router that is running NAT may corrupt the IP header checksum for some RTSP packets.

Conditions: This symptom is observed when the RTSP connection goes through NAT, “OPTION” or “DESCRIBE” messages are sent, and the NAT translation used has a differing number of characters for the private and public IP addresses of the server.

Workaround:

- 1) Configure the **no-payload** command for the NAT translation. This will stop the corruption, but will also cause all deep packet NAT to stop, which can cause other issues.
- 2) Use a port other than 554 for the RTSP steam. This will stop the corruption, but will also stop the router from NAT the embedded IP addresses in the RTSP packets. Depending on the specific implementation of RTSP, this may or may not stop the stream from working.
- 3) Change your NAT translation such that the private and public IP addresses have the same number of characters. For instance 192.168.0.1 has 11 characters, and 172.16.100.200 has 14 characters.

- CSCsw28501

Symptoms: After some time (days to months), all inbound and outbound calls through gateway fail with CCAPi cause 102. Calling party (PSTN or VoIP side) hear fast busy. When failure occurs, all calls, inbound and outbound fail. No R2 signaling is observed on inbound or outbound calls

Conditions: Observed with Cisco IOS Release 12.4.12c.

Topology: UCM/IP phones --- ip/h323 --- 5350 --- E1R2

No changes to network or gateway between incidents.

Workaround: Reboot gateway resolves issue for some time, issue returns after days or months.

- CSCsw98414

Symptoms: The **ip nat inside source ... match-in-vrf** command is not working without the *overload* option.

Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T8.

Workaround: There is no workaround.

- CSCsx03120

Symptoms: When an ATM interface on a WIC1-ADSL comes back up after a flap, under some undefined circumstances, it may be observed that none of the configured PVCs forward traffic.

Conditions: Specific conditions are still under investigation.

Workaround: Perform a **shut/no shut** on the interface or power cycle the router.

- CSCsx20984

Symptoms: Router reloads with a bus error and no tracebacks.

Conditions: Unknown at this time.

Workaround: There is no workaround.

- CSCsx52269

Symptoms: Switch port (Fa2 - Fa9) on Cisco 1812 pads an extra byte.

Conditions: Occurs when Cisco 1812 receives the packet with padding byte.

Workaround: There is no workaround.

- CSCsx69052

Symptoms: Service policy in suspend mode.

Conditions: The dLFloATM feature is configured on a Cisco 7500 and an attempt is made to attach policy to VT. The VT bandwidth is more than the required bandwidth of the policy.

Workaround: There is no workaround.

- CSCsx73372

Symptoms: Continuous DSP crash on Cisco 2801 router.

Conditions: Occurs on routers running Cisco IOS Release 12.4(23.15)PI10 and Cisco IOS Release 12.4(23.15)T5.

Workaround: There is no workaround.

- CSCsx81957

Symptoms: Router crashes due to memory corruption in TPLUS process.

Conditions: Occurs during normal operations.

Workaround: There is no workaround.

- CSCsy33492

Symptoms: Routing Information Base (RIB) and Cisco Express Forwarding (CEF) miss Open Shortest Path First (OSPF) external routes.

Conditions: Occurs when OSPF changes over to second path because first path interface is down.

Workaround: Enter the **clear ip route x.x.x.x** command.

- CSCsy40745

Symptoms: After disabling SSH, an alternate SSH port is still enabled on the router.

Conditions: Occurs on routers that have been configured to use a port other than Port 22 for SSH.

Workaround: Do not configure alternate SSH ports.

- CSCsy56320

Symptoms: If a T1/E1 controller on NM-CEM-4TE1 CEF module is configured for **clock source internal** so that it gets its clocking reference from the TDM backplane of a Cisco 2800 or 3800 Integrated Services Router (ISR), and the CEM T1/E1 controller flaps DOWN and then UP, the NM-CEM-4TE1 may cease being synchronized to the TDM backplane. Measurement and comparison of the clocking between the TDM backplane and the CEM T1/E1 shows that timing slips are occurring.

Conditions: This behavior may be observed on a Cisco 2800 or 3800 ISR which has been installed with a NM-CEM-4TE1 CEF module, and is running an IOS release from the 12.4 mainline train. The CEM T1/E1 controller is set for **clock source internal**.

Workaround: Two workarounds are known:

(1) Manually set **clock source line** and then **clock source internal** under the CEM T1/E1 controller. The CEM T1/E1 controller and the TDM backplane will be in synchronization from this point forward until the next T1/E1 flap.

(2) This behavior is not known to affect Cisco IOS Release 12.4T release. If Cisco IOS Release 12.4T can be deployed, use a current release of this train.

- CSCsy60426

Symptoms: High CPU utilization occurs when editing the ACL entries on a router running the c7301-ik9s-mz.124-23 image. The problem does not exist in the c7301-ik9s-mz.123-23 image.

Conditions: Occurs when two Cisco 7301 routers are configured for VPN redundancy. **crypto dynamic-map** is configured with match address to match crypto ACL that has 215 ACL entries. There are 1300 IPSec tunnels. Active router is running 7301-ik9s-mz.124-23, and standby router is running c7301-ik9s-mz.123-23.

The HIGH CPU problem is reported only on the router that is running 7301-ik9s-mz.124-23:

```
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 95%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
148 1085948 1402983 774 98.49% 97.28% 93.63% 0 Crypto IKMP
149 44592 86808 513 0.00% 0.00% 0.00% 0 IPSEC keyengine
```

The following steps reveal the problem:

- * There is a named ACL configured in the VPN router which defines the interesting traffic criteria for the establishment of the IPSec tunnel.
- * Enter configuration mode and add or remove entries from the named ACL.
- * Exit configuration mode. CPU utilization goes up to 99% momentarily on the router running Cisco IOS Release 12.3. After 4 seconds it returns to normal. On the router running Cisco IOS Release 12.4, CPU utilization stays high and affects router operations.

Workaround: Shift the tunnels over to the standby VPN by lowering the HSRP priority manually in the problematic router.

- CSCsy89234

Symptoms: Stateful Fail-over of Network Address Translation (SNAT) in primary/backup mode does not converge.

Conditions: Occurs after a **no shut interface** following a router reload, and then configure SNAT on the primary router.

Workaround: Perform a **shut/no shut** of the SNAT interface on the primary router.

- CSCsy92205

Symptoms: CPUHOG occurs due to tag control and crash in “atm_get_vc or atm_getvcnum”.

Conditions: Occurs on a Cisco 7500 with **mpls atm multi-vc** or **tag-switching atm multi-vc** configured.

Workaround: There is no workaround.

- CSCsz02943

Symptoms: Stateful fail-over of network address translation (SNAT) in primary/backup mode does not converge when TCP connect is shut down and then turned back on.

Conditions: It is seen with SNAT in primary/backup mode. Before the following conditions, both primary/backup routers is fully converged once.

1. Shutdown the SNAT interface of primary router and reload the primary router. Perform a **shutdown** on the SNAT interface of the primary router.
2. Shutdown the interface of the switch between SNAT routers. After 5 minutes, the SNAT peer is down. Enter **no shutdown** on the interface of the switch.

Workaround: Perform **shut/no shut** on the SNAT interface of the primary router.

- CSCsz21626

Symptoms: Reverse SSH session to TTY line with failed authentication results in occupied VTY line that will not clear.

Conditions: Occurs on a router running Cisco IOS Release 12.4(23) and earlier releases and with modem TTY lines configured to be accessed via reverse SSH session.

Workaround: Configure the router to use reverse telnet instead of reverse SSH. To clear a hung line, reload the router. If possible, run Cisco IOS Release 12.4T on the router to avoid the issue.

Resolved Caveats—Cisco IOS Release 12.4(25)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(25). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(25). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCec87860

Symptom: The IP Input Process holds large amounts of memory. The show mem allocating-process shows many TCL and ESM entries for IP Input.

Condition: ESM (Embedded Syslog Manager) is used under abnormally high logging conditions. The memory leak occurred in a test environment by logging every ACL denial, and pinging the denied interface in flood mode with 100,000+ packets.

Workaround: Do not use ESM if experiencing abnormally high syslog traffic.

- CSCek48205

Symptoms: The output counters for a Multilink Frame Relay (MFR) bundle interface may not be updated correctly.

Conditions: Occurs after the same interface is deleted and recreated.

Workaround: There is no workaround.

- CSCsc77638

Symptoms: Using a 3725 with an AIM-ATM/VWIC-2MFT-T1 combo, running the following IOS releases may result in ATM PVCs configured with VCIs greater than 255 to fail.

Conditions: Occurs when using a Cisco 3725 with AIM-ATM, VWIC-2MFT-T1, and the c3725-jsx-mz.123-14.T2 image with an HDLC channel-group configured on 1/2 VWIC ports with the other port using the AIM-ATM SAR.

Workaround: Use VCIs less than 255 or remove Channel-Group sharing VWIC with AIM-ATM.

- CSCsc78999

Symptoms: An Address Error exception occurs after Uninitialized timer in TPLUS process.

Conditions: This is a platform independent (AAA) issue. It may be seen with a large number of sessions while accounting is configured with a T+ server.

Workaround: Disable accounting, or use RADIUS accounting instead of a T+ server.

- CSCsd09324

Symptoms: When reloading a router (lsnt-ap-pe1, Cisco 7500 platform) with Cisco IOS interim Release 12.0(31.4)S1 from any Cisco IOS Release 12.0(28)S4b image, several IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP and traceback occur in the standby log.

Conditions: This symptom has been observed on a Cisco 7500 router platform with MVPN.

Workaround: There is no workaround.

- CSCsg09423

Symptoms: When IPsec SAs flap, traffic loss may occur during the IPsec and IKE rekey.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when there is a large number of IKE and IPsec SAs (that is, more than 2000 IKE SAs and 4000 IPsec SAs) and when RSA signature authentication is configured.

Workaround: Reduce the number of IKE and IPsec SAs.

- CSCsg84765

Symptoms: A MWAM-SSG processor may reload automatically with the following error message:

%ALIGN-1-FATAL: Corrupted program counter pc=0x0 , ra=0x21A8C118 , sp=0x45E7D7D0

Conditions: The symptom is observed with MWAM in a Cisco 7600 series router that is running Cisco IOS Release 12.4(3b).

Workaround: There is no workaround.

- CSCsi17158

Symptoms: Devices running Cisco IOS may reload with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

Conditions: This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

Workaround: There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with “ssh” removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

More information on configuring ACLs can be found on the Cisco public website:

<http://www.cisco.com/warp/public/707/confaccesslists.html>

- CSCsi25562

Symptoms: Cisco 2600XM router runs out of memory while trying to boot large images.

Conditions: This defect produces crashes under two scenarios:

1.) During loading of large images, such as a c2600-adventerprisek9-mz.
2.) During reload where router goes into ROMMon.

Workaround: There is no workaround.

- CSCsi41062

Symptoms: A Standby router will reload with the following error message:

02:05:27: Config Sync: Line-by-Line sync verifying failure on command: cbr 2000 due to parser return error

Conditions: This issue is seen when CBR service category is configured on VC on CEoP IMA i/f.

Workaround: There is no workaround.

- CSCsi47635

Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCsi95862

Symptoms: Router crashes when the **mobile router-service roam priority** command is entered.

Conditions: Crash is observed during unconfiguration after verifying for generic routing encapsulation.

Workaround: There is no workaround.

- CSCsj17304

Symptoms: A multicast source address may not get translated if the Network Address Translation (NAT) outside the interface is a GRE tunnel.

Conditions: The symptom is observed when using NAT to translate a multicast source address for multicast traffic over a tunnel interface. The static NAT translation of the multicast source address does not work.

Workaround: Turn off CEF globally on the router.

Alternate workaround: Turn off the mroute-cache on the NAT inside the interface.

- CSCsj36133

Symptoms: A BGP neighbor may send a notification reporting that it received an invalid BGP message with a length of 4097 or 4098 bytes.

Conditions: The problem can be seen for pure IPv4 BGP sessions (no MP-BGP in use) when the router that is running the affected software generates a large number of withdraws in a short time period and fills an entire BGP update message (up to 4096 bytes normally) completely with withdraws. Because of a counting error, the router that is running the affected software can generate an update message that is 1 or 2 bytes too large when formatting withdraws close to the 4096 size boundary.

Workaround: The issue is not seen when multiple address families are being exchanged between BGP neighbors.

- CSCsj46707

Symptoms: A CPU may hang and give traceback during boot up.

Conditions: The crash is the result of a race condition caused by the order of operations in console_init().

Workaround: There is no workaround.

- CSCsk22496
Symptoms: Spurious access or a router crash may be seen when a crypto key is removed.
Conditions: The crypto key was not generated in the router. When we try to remove the unconfigured crypto key, the spurious access may be seen.
Workaround: There is no workaround.
- CSCsk72676
Symptoms: PVC does not come up after removing vc-class from it.
Conditions: This issue happens only when vc-class with constant bit rate (CBR) is configured on the main interface, and another vc-class is applied to the VC. This occurs under the following scenario:
 1. Boot the router afresh.
 2. Apply a vc-class (class1) to the ATM interface.
 3. Configure PVCs with the range command.
 4. Apply another vc-class (class2) under the range-pvc configuration.
 5. Remove the vc-class (class2) from under the range-pvc configuration.
 After this step the PVCs are expected to come up having attributes of vc-class class1. The PVCs do not come up and stay in inactive mode.
Workaround: There is no workaround.
- CSCsm56940
Symptoms: Traceback seen while doing Telnet with SSH enabled.
Conditions: Occurs when SSH is enabled on a Cisco 7200 router.
Workaround: There is no workaround.
- CSCsm75818
Symptoms: Multicast data loss may be observed while changing the PIM mode of MDT-data groups in all core routers.
Conditions: The symptom is observed while changing the PIM mode of MDT-data groups from “Sparse” to “SSM” or “SSM” to “Sparse” in all core routers in a Multicast Virtual Private Network (MVPN).
Workaround: Using the command **clear ip mroute MDT-data group** will resolve the issue.
- CSCsm97220
Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.
Cisco has released free software updates that address these vulnerabilities.
This advisory is posted at the following link
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>
- CSCso87348
Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. Additionally, this single bug can affect T train platforms on limited releases as detailed below.
Conditions: Occurs when NetFlow is configured on one of the following:
 - * Cisco 7600 running Cisco IOS Release 12.2(33)SRC. * Catalyst 6500 running Cisco IOS Release 12.2SXH.

Workaround: Disable NetFlow. This is done with the following commands:

no ip flow ingress no ip flow egress no ip route-cache flow

Enter the appropriate command for each subinterface for which NetFlow is currently configured.

Other Notes:

12.4(23) is affected by this bug. The fix is in releases thereafter for 12.4.

The 12.2SRC and 12.2SXH code trains are affected. The specific versions affected are 12.2(33)SXH, 12.2(33)SXH1, 12.2(33)SXH2, 12.2(33)SXH2a, 12.2(33)SRC, and 12.2(33)SRC1

The issue is fixed in the two affected code trains from the 12.2SXH3 and 12.2SRC2 releases onwards. However, for the SXH train, Cisco would recommend the use of SXH4 due to bug CSCso71955

The following release trains do not have this issue; 12.2(18)SXF, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXI and all other release trains after those affected.

- CSCso90058

Symptoms: MSFC crashes with RedZone memory corruption.

Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

Workaround: There is no workaround.

- CSCsq23391

Symptoms: Memory leak was found after voice stress testing on a Cisco 3845.

Conditions: Occurred on router configured for E1, Direct Inward Dial (DID), G.711, and voice activity detection (VAD). Testing was performed for 2 hours, and call duration was 60 seconds.

Workaround: There is no workaround.

- CSCsr18173

Symptoms: 1. If dampening is enabled on a router, and identical updates of a IPv4 prefix carrying label information are received, these updates are not treated as identical and dampening penalty is set for the route. 2. If dampening is enabled on a router, and identical updates of a IPv4 multicast prefix are received, these updates are not treated as identical and dampening penalty is set for the route.

Conditions: The symptom is observed when dampening is enabled and: 1. Identical updates of a IPv4 prefix are received. The updates should be carrying MPLS Label information; or 2. Identical updates of a IPv4-multicast prefix are received.

Workaround: There is no workaround.

- CSCsr25788

Symptoms: Output drops can be observed on GE/FE interface on a Cisco 2800 router.

Conditions: Problem is observed when NAT is enabled while router is configured to pass multicast traffic.

Workaround: There is no workaround.

- CSCsr59242

Symptoms: EIGRP may lose some routes from stub neighbors in a DMVPN setup.

Conditions: If EIGRP graceful restart happens on an interface and the interface update queue is busy, then it may lose some routes from the stub neighbors on that interface.

For example, issuing the below commands can trigger this issue:

clear ip eigrp vrf abc as-number neighbors interface Wait 30 seconds **clear ip eigrp vrf abc as-number neighbors interface soft**

Workaround: Use the **clear ip eigrp vrf abc neighbors** command to fix the problem.

Another workaround is that graceful restart can be turned off by the **no eigrp graceful-restart** command under the router or the **address-family** command. This will cause the symptom to go away but will revert back to hard resetting peers on configuration changes or the **clear ip eigrp neighbor soft** command.

- CSCsr61125

Symptoms: A switchover takes more time on a Cisco 7500 router.

Conditions: This symptom is observed when RPR+ is configured on the Cisco 7500.

Workaround: There is no workaround.

- CSCsr74295

Symptoms: Upon reload, static routes pointing to MLPPP interfaces do not get inserted in the RIB.

Example: **ip route 172.16.2.2 255.255.255.255 multilink22**

Conditions: Occurs in a router running Cisco IOS Release 12.2(33)SRC1.

Workaround: Reconfigure the static routes being affected, or simply configure **copy run start** to initialize the routes.

- CSCsr80601

Symptoms: An ISAKMP SA is not deleted as expected after removing the RSA key.

Conditions: The issue is seen when the user tries to clear the ISAKMP SAs by issuing the **clear crypto session** command on an IKE SA that has multiple IPSEC SAs.

Workaround: Use the **clear crypto sa** and **clear crypto is** commands.

- CSCsr90248

Symptoms: Changing any of the parameters of a route-map does not take effect.

Conditions: Occurs when using a BGP aggregate-address with an advertise map.

Workaround: Delete the aggregate-address statement and then put it back for the change to take effect.

- 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.

- CSCsu04446

Symptoms: A Cisco router that is running a PfR Master Controller crashes under stress.

Conditions: This symptom is observed when traffic with more than 2000 prefixes with about 500 unreachable prefixes is flowing through the router.

Workaround: Minimize the number of prefixes learned during an interval. The default of 100 should be sufficient.

- oer master learn prefixes 100
- CSCsu10229

Symptoms: cdpCacheAddress(OID:1.3.6.1.4.1.9.9.23.1.2.1.1.4) MIB is not showing GLOBAL_UNICAST address.

Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T7.

Workaround: There is no workaround.
 - CSCsu18232

Symptoms: When a port becomes active the endpoints stay in “Not Ready” state and the RSIP message is not sent.

Conditions: The symptoms are observed when a new E1/T1 is configured with new DS0 groups controlled by MGCP. It is observed only during initial configuration.

Workaround: Remove the entire configuration under the controller before reloading/configuring a new set. After the problem occurs, the only workaround is to reload router.
 - CSCsu20376

Symptoms: When a user configures the **exception flash all disk1:core1** command, the resulting coredump pathname becomes “disk1:core1:ram1-7206-2-coreiomem.Z”. The presence of the “:” following core1 is bogus since “:” is a reserved character used to delimit device and partitions. And “core1” is not a valid partition identifier.

A reasonable interpretation of “core1” would be as an existing subdirectory, not as the first 5 characters of a core file name.

Conditions: Occurs when user configures the **exception flash all disk1:core1** command.

Workaround: Copy the core dump to “disk1:” instead of “disk1:core1”. Use “exception flash all disk1:”
 - CSCsu25833

Symptoms: An ISR router may crash with the following error message: %ALIGN-1-FATAL: Corrupted program counter

Conditions: The symptoms are observed on a Cisco 2811 and 2801 router. The trigger has not yet been identified.

Workaround: There is no workaround.
 - CSCsu26174

Symptoms: A Cisco 1800 series router may stop passing traffic on FastEthernet interface 0/1 when FastEthernet interface 0/0 is administratively shut down using the interface configuration command **shutdown**. When FastEthernet 0/0 is shutdown, the following message is displayed:

```
%GT96K_FE-5-LATECOLL: Late Collision on int FastEthernet0/0
```

Conditions: The symptoms are observed with FastEthernet 0/0 on a Cisco 1841 router and when the device at the far end of interface FastEthernet 0/0 is configured manually to speed 10 or 100.

Workaround: Configure the far-end device to auto-negotiate the speed with the 1800 router.

Further Problem Description: This problem does not occur when pulling out cable and re-inserting in FastEthernet 0/0. It also does not occur when FastEthernet 0/1 is reversed to FastEthernet 0/0.
 - CSCsu27888

Symptoms: IGMP v3 reports are discarded.

Conditions: Occurs on Cisco 7200 router running Cisco IOS Release 12.4(20)T2.

Workaround: There is no workaround.

- CSCsu29158

Symptoms: A class map with an interface defined is lost in the new standby.

Conditions: Configure a Cisco 7500 for RPR+ mode. Configure a class map with an input interface. Do an OIR remove the slot, and then a switchover. OIR Insert the slot in the new master. The new standby will not have the match statement for the input interface.

Workaround: Reload the standby once again.

- CSCsu29526

Symptoms: Customer seeing memory corruption crash on his device while doing NAT protocol translation from IPv4 to IPv6

Conditions: System was restarted by error - an unknown failure

Workaround: Apply the following to the configuration:

no ipv6 nat service dns

Note that there will not be IP address translation in DNS packets going between IPv6 and IPv4 network.

- CSCsu35597

Symptoms: Renaming a directory gives error message.

Conditions: This happens on a Cisco router running Cisco IOS Release 12.4(20)T1.fc2 image

Workaround: There is no workaround.

- CSCsu36836

Symptoms: TCL scripts and policies attempting to work with open files and sockets simultaneously may not operate properly. One symptom is the **vwait** command may fail by reporting “would wait forever”.

Conditions: Occurs when a TCL script opens both a file and a client or server socket simultaneously.

Workaround: Open and close files and sockets separately. Avoid having them open simultaneously.

- CSCsu37317

Symptoms: A Cisco 7500 router crashes.

Conditions: IMA interface is configured with three and four members each. Attach service policy to an IMA pt interface. Now try to remove the IMA pt interface.

Workaround: There is no workaround.

- CSCsu41968

Symptoms: On a Cisco 7500 with an HA setup, the “show controller t3” command is showing framing as M23 on the active and as C-bit on the standby. So the “loopback remote” configuration is rejected on the active and is accepted on the standby.

Conditions: This symptom is observed when the “show controller t3 1/1/0” command is issued.

Workaround: There is no workaround.

Further Problem Description: Because of the framing mismatch, the standby might crash due to sync issues.

- CSCsu44696

Symptoms: A Cisco 7500 series router may crash.

Conditions: The symptom is observed when trying to access the VIP console when it is about to crash.

Workaround: There is no workaround.

- CSCsu44789

Symptoms: Spurious memory access traceback is seen.

Conditions: The symptom is observed when an MGCP Gateway tries to defer a Request Notification (RQNT) without the requested/signal event.

Workaround: There is no workaround.

- CSCsu45425

Symptoms: Label Forwarding Information Base (LFIB) shows incorrect information for Global BGP prefix after route flap. LFIB/FIB shows prefix as having a tag when it should be not. Routing table is correct.

Conditions: Occurred on a Cisco 12000 router running Cisco IOS Release 12.0(33)S1.

Workaround: Enter the **clear ip route** command.

- CSCsu45780

Symptoms: The following error message is displayed if the DSU bandwidth is configured with a value other than the default of 44210 for T3 on an NM-1T3/E3 module:

```
dsxpnm_gt96k_abort_tx_mpsc:Aborting Tx mpsc failed
```

Conditions: The symptom is observed when the DSU bandwidth is changed to a value other than the default of 44210. It mostly occurs with values below 1000.

Workaround: Leave the DSU bandwidth at the default of 44210.

- CSCsu48898

Symptoms: A Cisco 10000 series router may crash every several minutes.

Conditions: The symptom is observed with a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB13.

Workaround: Use Cisco IOS Release 12.2(31)SB11.

- CSCsu63996

Symptoms: NSF restart may be terminated and OSPF NBR may flap during RP switchover. The **debug ip ospf adj** command shows the following message: OSPF: Bad request received.

Conditions: The symptoms are observed when the links are broadcast networks and the restarting router is DR. It is seen when “nsf cisco” is configured and when some neighbors finish OOB resync much sooner than others.

Workaround: Use the **nsf ietf** command.

Alternate workaround: Configure routers so that the restarting router is not DR (use ospf network type point-to-point or priority 0).

- CSCsu65189

Symptoms: If router is configured as follows:

```
router ospf 1 ... passive-interface Loopback0
```

And later is enabled LDP/IGP synchronization using command

```
Router(config)#router ospf 1 Router(config-router)# mpls ldp sync
Router(config-router)#^Z
```

MPLS LDP/IGP synchronization will be allowed on interface loopback too.

```
Router#sh ip ospf mpls ldp in Loopback0 Process ID 1, Area 0 LDP is not configured
through LDP autoconfig LDP-IGP Synchronization : Required < ---- NOK Holddown timer is
not configured Interface is up
```

If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

Workaround: Do not configure passive loopback under OSPF. Problem only occurs during reconfiguration.

The problem will not occur if LDP/IGP sync is already in place and: - router is reloaded with image with fix for CSCsk48227 - passive-interface command is removed/added

- CSCsu73571

Symptoms: VIP may crash on a Cisco 7500 series router.

Conditions: The symptom is observed when Distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) or Distributed Link Fragmentation and Interleaving over ATM (dLFIoATM) is configured and “ip flow egr” is configured on multilink or VT.

Workaround: There is no workaround.

- CSCsu74397

Symptoms: When removing PA-MC-8TE1+ from the chassis, the router has an unexpected system reload. This reload happens when you remove the port adapter and the router is running the Cisco IOS bootloader image. Also happens when the port adapter is removed after the router finishes loading the Cisco IOS bootloader image and before it loads the complete Cisco IOS Software image.

Conditions: This occurs on a Cisco 7200 VXR NPE-G2 Series Routers on the Cisco IOS bootloader image from the Cisco IOS Release 12.4(4)XD.

Workaround: Remove PA-MC-8TE1+ when the complete Cisco IOS Software Image finishes loading.

- CSCsu74400

Symptoms: A device running FTP to transmit the DHCP database may experience a file descriptor leak that results in errors such as:

```
ROUTER#show run
```

OR

```
ROUTER#show start Using XXXX out of XXXX bytes %Error opening nvram:/startup-config
(Bad file number)
```

OR

```
ROUTER#dir nvram: Directory of nvram:/ %Error opening nvram:/ (File table overflow)
XXXX bytes total (XXXX bytes free)
```

Conditions: Occurs when the router is configured to use FTP to transmit the DHCP database:

```
ip dhcp database ftp://XXXX:XXXX@X.X.X.X/XXXX
```

And the FTP server becomes unreachable. The file descriptor leak can be viewed in the output of **show file descriptors**:

```
ROUTER-B#show file descriptors File Descriptors:
```

```
FD Position Open PID Path 0 0 0302 145 ftp://X.X.X.X/DHCP 1 0 0302 145
ftp://X.X.X.X/DHCP 2 0 0302 145 ftp://X.X.X.X/DHCP 3 0 0302 145 ftp://X.X.X.X/DHCP 4 0
0302 145 ftp://X.X.X.X/DHCP 5 0 0302 145 ftp://X.X.X.X/DHCP 6 0 0302 145
ftp://X.X.X.X/DHCP 7 0 0302 145 ftp://X.X.X.X/DHCP 8 0 0302 145 ftp://X.X.X.X/DHCP 9 0
0302 145 ftp://X.X.X.X/DHCP <snip>
```

Workaround: Ensure that the FTP server does not become unreachable for more than 128 total minutes, as there are only 128 file descriptors. In the event that all 128 file descriptors are leaked, a reboot is required to recover.

- CSCsu76993

Symptoms: EIGRP routes are not tagged with matching distribute-list source of route-map.

Conditions: Problem is observed where the route-map is applied to a specific interface. When the route-map is applied globally without the specific interface things appear to work fine.

Workaround: There is no workaround.

- CSCsu79754

Symptoms: PIM packets may be processed on interfaces which PIM is not explicitly configured.

Conditions: Unknown at this time.

Workarounds: Create an ACL to drop PIM packets to such interfaces.

- CSCsu92432

Symptoms: The router's async line used for reverse SSHv2 might hang after a failed authentication and not recover unless the router is rebooted. The router log displays: %SYS-3-HARIKARI: Process SSH Process top-level routine exited

Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4 with async lines.

Workaround: Use the traditional way of using reverse SSH with the use of rotaries.

- CSCsu95080

Symptoms: A router remains in the init_process state when parsing the configuration.

Conditions: The symptom is observed when an IPv6 multicast group joins without MLD configured. When the groups unjoin, the system suspends.

Workaround: Configure MLD.

- CSCsv00168

Symptoms: Junk values are being displayed on the router when characters/commands are inputted. For example, enter "enable", it shows "na^@^@"; enter "show version", it shows "h^v^@e^@^r^@^@^@^@^@".

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.

- CSCsv01474

Symptoms: The **ip rip advertise** command might be lost from the interface.

Conditions: This symptom occurs in any of the following three cases:

1. The interface flaps. 2. The **clear ip route** command is issued. 3. The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

Workaround: Configure the **timers basic** command under the address-family under rip.

- CSCsv03300

Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard gigabitethernet interface.

Workaround: There is no workaround.

- CSCsv04275

Symptoms: The **show logging** command displays messages such as the following:

```
<date>: %ATM_AIM-5-CELL_ALARM_UP: Interface ATM<if ID> lost cell delineation. <date>:
%ATM_AIM-5-CELL_ALARM_DOWN: Interface ATM<if ID> regained cell delineation.
```

The link may go down and then recover automatically.

Conditions: This symptom is observed under ordinary operation. There is no apparent trigger. The physical line is known to be good.

Workaround: There is no workaround.

- CSCsv04836

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- CSCsv06608

Symptoms: SXP is set up between two devices but fails to initialize.

Conditions: This symptom is observed when SXP is set up between two devices.

Workaround: There is no workaround.

- CSCsv15266

Symptoms: A router that is running Cisco IOS Release 12.4 with QoS configured with a parent and child policy may experience a reset due to a software-forced crash displaying one of the following messages:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
dealloc XXXXXXXX
```

OR

```
%SYS-6-BLKINFO: Corrupted magic value in in-use block blk XXXXXXXX, words XX, alloc
XXXXXXXX, Free, dealloc XXXXXXXX, rfcnt X
```

Conditions: The reset is triggered by a configuration change tied to QoS and has been seen while changing one of the following:

- An access-list referenced by the map-class.
- The DSCP/Precedence values being set by the service-policy.
- Removing the service-policy from the interface.
- Altering the shaping parameters within the service-policy.

Workaround: Other than avoid making changes to the QoS outside of a maintenance window, there is no workaround.

- CSCsv20948

Symptoms: The primary router may crash continually.

Conditions: The symptom is observed with two Cisco 3825 routers with the same software and hardware and with a situation where one is working as a primary router and the other as a secondary. The issue is seen only with voice traffic. It is observed when running Cisco IOS Release 12.4(20)T (with this release the primary router crashes very frequently) and also with Cisco IOS Release 12.4(20)T1.

Workaround: There is no workaround.

- CSCsv27480

Symptoms: VRRP virtual MAC address is stored as a dynamic, instead of static, entry after a reload.

Conditions: The symptom is observed when VRRP is configured on an SVI with xconnect pseudowire:

```
interface Vlan X ip address 10.0.0.1 255.255.255.0 vrrp 2 ip 10.0.0.254 xconnect vfi
VRRP_3201
```

Workaround: Use the **shutdown** followed by the **no shutdown** commands on the SVI (VLAN interface).

- CSCsv27607

Symptoms: BGP router filters outbound routes to the peers when doing soft reset with specifying peer address using the **clear ip bgp ip-addr soft out** command. However, the routes to be filtered are not deleted from the routing table on the BGP peer router.

Conditions: The symptom happens when removing and then reapplying an outbound route-map. When issuing the **clear ip bgp neighbor-address soft out** command for each peer in an update-group after applying the outbound route-map filtering policy. The withdraw for filtered prefixes is sent to the first peer specified in soft reset, but the next peers in the same update-group do not withdraw the routes.

Workaround: Perform a hard BGP reset using the **clear ip bgp ip-addr** command.

- CSCsv28806

Symptoms: When a dspfarm profile still has active calls, if the user manually shuts down the dspfarm profile, the router will crash.

Conditions: The user manually shuts down a dspfarm profile when it is still in use with active calls. This includes the case where a dspfarm profile is manually shut down after a DSP crash occurs to the dspfarm service but the endpoint phones have not yet finished hanging up.

Workaround: Do not shut down a dspfarm profile if it is still in use by active calls. Besides, if a DSP crash occurs, hang up all the phones using that dspfarm service and wait until the DSP sessions are released before manually shutting down the dspfarm profile.

- CSCsv30075

Symptoms: A Cisco router may reload due to a bus error.

Conditions: This symptom has been experienced on a Cisco router that is running Cisco IOS Release 12.4(15)T7 and that is configured with NAT.

Workaround: There is no workaround.

- CSCsv34305

Symptoms: A router may crash while configuring **snmp mib community-map comm engineid** with a long word.

Conditions: The symptom is observed with a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T.

Workaround: There is no workaround.

- CSCsv36187

Symptoms: There may be a crash following a warning of an uninitialized timer.

Conditions: Pushing configuration to the device from a CE has been demonstrated to cause this. However, this does not always cause a crash.

Workaround: There is no workaround.

Further Problem Description: Configuration via interactive CLI is not subject to this fault.

- CSCsv38166

The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>.

- CSCsv38205

Symptoms: Running a post-dial delay operation with reaction configuration may cause a router to crash after removing the operation.

Conditions: The symptom is observed when using a post-dial delay operation with reaction configuration.

Workaround: Do not use reaction configuration for post-dial delay.

- CSCsv38804

Symptoms: VIC2 BRI Layer 2 will not come up after boot up.

Conditions: The symptom is observed with VIC2-2BRI-NT/TE cards.

Workaround: There is no workaround.

- CSCsv40404

Symptoms: When DDNS is disabled on the router which is configured as the DHCP server, it sends option 81 in the DHCP ACK message with the N flag bit set to 1. However, the DHCP client fails to understand this and will not undertake a PTR update.

Conditions: The issue is seen with a third-party vendor DNS server and a Cisco IOS DHCP server.

Workaround: There is no workaround.

Further Problem Description: The issue is not seen with the 12.3 code as it does not support DDNS and hence does not reply back with Option 81 in the DHCP ACK.

- CSCsv40902

Symptoms: The CBAC (**ip inspect**) commands are missing.

Conditions: The symptom is observed with Cisco IOS interim Release 12.4(23.5) CLI.

Workaround: There is no workaround.

- CSCsv42636

Symptoms: A Cisco 1721 reloads due to a bus error.

Conditions: The symptom is observed on a Cisco 1721 which is configured for AAA and is running Cisco IOS Release 12.4(16a), 12.4(16b) and 12.4(21). This is a platform independent issue and can possibly be seen on other platforms.

Workaround: There is no workaround.

- CSCsv45669

Symptoms: EIGRP fails to send updates via the dialer when the ATM interface is flapped.

Conditions: The symptom is observed in a PPPoATM setup with cloned virtual-access subinterfaces and an EIGRP neighbor established over that PPPoATM connection. When the ATM interface carrying the PVC in use for the PPPoATM session is shutdown and reenabled after the EIGRP neighbor and PPPoATM session have timed out, we see a problem with reestablishing the EIGRP neighborship.

Workaround: In global configuration mode, use the following command: **no virtual-template subinterface**. This instructs the router to clone only the main interfaces, not the virtual-access subinterfaces.

- CSCsv50666

Symptoms: While lrq forward-queries is configured, the gatekeeper blasting does not work as expected.

Conditions: This symptom is observed when lrq forward-queries is configured.

Workaround: There is no workaround.

- CSCsv50958

Symptoms: A router reloads when DTMF digits are dialed out while making an MGCP call.

Conditions: This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.4(23.5).

Workaround: No workaround is known.

- CSCsv52459

Symptoms: A Cisco device that is running Cisco IOS Release 12.3(7)T or later Cisco IOS code may see an increase in CPU usage when upgrading from a previous image.

Conditions: NAT must be enabled for the contributing factor described here to be applicable. RTSP and MGCP NAT ALG support was added, which requires NBAR. However, there is no way to disable it if that feature code is not needed.

Workaround: There is no workaround.

- CSCsv54130

Symptoms: Ping fails in HWIC-2T and WIC-2T when the physical mode is changed to “Async” from “Sync” with PPP encapsulation.

Conditions: The symptom is observed when the initial configuration is in Sync mode as shown:

```
interface Serial0/1/0 ip address x.x.x.x 255.0.0.0 encapsulation ppp end
```

Then the configuration is changed to Async mode:

```
Current configuration: 123 bytes ! interface Serial0/1/0 physical-layer async ip address x.x.x.x
255.0.0.0 encapsulation slip async mode dedicated end
```

Workaround: Toggling the encapsulation to PPP sometimes fixes the issue. This may have to be done multiple times until the interface comes up.

- CSCsv54510

Symptoms: The router is not getting pruned after shutting the interface. The pruned flag is not getting set even after waiting for long time.

Conditions: Happens with a Cisco 7200 router running Cisco IOS Release 12.4(24)T.

Workaround: There is no workaround.

- CSCsv59334

Symptoms: Upon entering the configuration command **no network 0.0.0.0 0.0.0.0** under the eigrp router configuration mode, all the EIGRP routes that were redistributed get withdrawn.

Conditions: The symptom is observed when using explicit network prefixes as well as network 0.0.0.0/32 which includes unspecified, directly connected networks to enable EIGRP on various interfaces of a router. These EIGRP routes are also redistributed into BGP. In such a case, on entering the configuration command **no network 0.0.0.0 0.0.0.0** under the eigrp router configuration mode, all the EIGRP routes that were redistributed get withdrawn. For example:

```
router eigrp 1 network 10.0.0.0 network 0.0.0.0 Rt130#sh ip eigrp topo EIGRP-IPv4
Topology Table for AS(1)/ID(10.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s
- sia Status
P 10.1.1.1/32, 1 successors, FD is 128256 via Connected, Loopback1 P 10.1.1.0/24, 1
successors, FD is 281600 via Connected, Ethernet1/0 P 10.147.204.64/26, 1 successors,
FD is 281600 via Connected, Ethernet0/2 P 10.147.204.0/26, 1 successors, FD is 281600
via Connected, Ethernet0/0
```

In the above configuration, network 10.0.0.0/24 is explicitly included under EIGRP by the network 10.0.0.0 configuration. The other networks (13, 20 etc) are included by the network 0.0.0.0 configuration. If EIGRP routes are redistributed into BGP, the three networks 10, 13 and 20 can be seen by BGP. On doing a **no network 0.0.0.0 0.0.0.0**, we would expect the redistribution of networks 13 and 20 to stop while network 10 continues to get redistributed. However, all the networks 10, 13 as well as 20 do not get redistributed into BGP.

Workaround: Clear the IP route and reload to allow the networks to get in the BGP table.

- CSCsv62777

Symptoms: A VTY session may get stuck after some extended pings are done and the CPU process may go high.

Conditions: The symptom is observed when an extended ping with CLNS is done and the command is left incomplete until the VTY session times out.

Workaround: Issue can be prevented by not leaving the extended **ping clns** command incomplete for long time in the VTY session.

- CSCsv65915

Symptoms: A Cisco 7500 series router configured with distributed or non-distributed CEF and WCCP, may redirect WCCP bypass packets back to the cache device resulting in a loop for this traffic.

Conditions: The symptom is observed with a Cisco 7500 series router with distributed or non-distributed CEF and WCCP.

Workaround: Disable CEF.

- CSCsv66827

Symptoms: Clearing the SSH sessions from a VTY session may cause the router to crash.

Conditions: The symptom is observed when a Cisco 7300 series router is configured for SSH and then an SSH session is connected. If the SSH session is cleared every two seconds using a script, the symptom is observed.

Workaround: There is no workaround.

- CSCsv73509

Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under VTY configuration.

Conditions: Configure “no aaa new-model”, configure login local under line VTY 0 4 and configure login tacacs under line VTY 0 4.

Workaround: There is no workaround.

- CSCsv77932

Symptoms: Router crashes.

Conditions: Occurs while configuring serial interface for insufficient MTU.

Workaround: There is no workaround.

- CSCsv78559

Symptoms: A first fragmented packet is matched unexpectedly by PBR when the router fragment the packets to transfer over a GRE tunnel.

Conditions: The symptom is observed under the following conditions:

- The router needs fragmentation to transport packets over the GRE tunnel. - when using the match statement for input interface on route-map of PBR and the interface matches with the GRE tunnel which is used for the output packet.

The router needs the fragmentation to transfer over the GRE tunnel.

Workaround: Disable fast-switching and configure “no ip route-cache” on the GRE tunnel.

Alternate workaround: Use “match ip address” instead of “match interface” on policy-map AND deny GRE packets on the ACL of the “match ip address” clause.

- CSCsv79584

Symptoms: An 0.0.0.0 binding with a 0 minute lease gets created and subsequently removed on the DHCP unnumbered relay.

Conditions: The DHCP client sends a DHCPINFORM with ciaddr set to its address, but giaddr is empty. The relay fills in giaddr with its IP address and the server replies to giaddr. Since the DHCPACK is in response to DHCPINFORM, the lease-time option is absent. Relay receives the DHCPACK and tries to process it normally leading to the route addition.

Workaround: There is no workaround.

Further Problem Description: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP requests. Examining “debug ip routing” for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv87146

Symptoms: Clearing of NAT translation either manually or automatically through timeout results in crash.

Conditions: Occurs when a dynamic translation mapping is removed while traffic is running.

Workaround: Stop traffic before removing dynamic NAT translation.

- CSCsv90106

Symptoms: A router may write a crashinfo that lacks the normal command logs, crash traceback, crash context, or memory dumps.

Conditions: This might be seen in a memory corruption crash depending on precisely how the memory was corrupted.

Workaround: There is no workaround.

- CSCsv91838

Symptoms: A router may crash and the following traceback may be seen:

```
Traceback= 0x6141BE68 0x6141CF74 0x6141E3F0 0x619D2A04 0x619D3150 0x619F8950
0x633C68D8 0x633C68BC
```

Conditions: The symptoms are observed on a Cisco 3825/3725 with WIC/HWIC ADSL/SHDSL cards and when the **atm video aesa default** command is executed on the ATM interface. It is seen with the c3825-adventerprisek9-mz.124-21.14.T1 and c3825-adventerprisek9-mz.124-23.7.T images.

Workaround: There is no workaround.

- CSCsv94099

Symptoms: Traceback may be seen in relay.

Conditions: The symptom is observed in an unnumbered scenario when the client releases the address.

Workaround: There is no workaround.

- CSCsv97772

Symptoms: The System Activity (SYS ACT) LED may keep blinking even though there are no configurations or traffic.

Conditions: The symptom is observed on a Cisco 2800 series router with an NM-16A/S, which is connected to another device through a CAB-SS-X21MT. The problem is only seen on a couple random ports on a few random modules.

Workaround: Use RS-232 cables instead of X.21 cables.

- CSCsv99335

Symptoms: If HTSP is NULL, using it to reference other data members will cause a traceback or may cause the router to crash.

Conditions: The symptom occurs when the condition enters into an offhook state and HTSP is NULL. It is very rare for HTSP to be NULL and is only detected by SA.

Workaround: There is no workaround.

- CSCsw18636

Symptom:

High CPU utilization after receives a ARP packet with protocol type as 0x1000.

Conditions: This problem occurs on SUP32 running 12.2(33)SXI. This problem may also occur on SUP720. The problem is only seen when you have bridge-group CLI being used which lead to arp pkts with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

Workaround: Filter the ARP packet. The device Config should have bridge-group creation first; followed by interface specific bridge-group options.

Additional-Info.

This problem is now isolated to command ordering in the startup-config file. bridge <> command is saved before bridge-group <> command (which is run in the interface-config mode) is saved. The linking of IDB to bridge structure is not happening correctly and some check fails in the bridge code that lets the packet to be processed again and again instead of being dropped.

If bridge-group <> command is removed in the startup-config and only applied after bridge <> command is run, problem will go away. Please use this workaround until a fix is put in.

- CSCsw21308

Symptoms: A router crashes when users try to access the “vc-class” at same time.

Conditions: The symptom is observed if an attempt is made to configure and remove the same vc-class using the different VTY or console terminals. The crash may be seen if one terminal has removed the class but it remains in another one. Under standard recommended IOS configuration procedure this issue will not be seen.

Workaround: There is no workaround.

- CSCsw23397

Symptoms: A Cisco Communication Media Module (CMM) may leak memory in the chunk manager.

Conditions: The symptom appears to be triggered by calls that disconnect prematurely.

Workaround: There is no workaround.

Further Problem Description: Though this problem is seen and reported on CMM, it may occur on any IOS gateway supporting voice (28xx, 38xx, 5xxx).

- CSCsw24542

Symptoms: A router may crash due to a bus error after displaying the following error messages:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error, %ALIGN-1-FATAL: Illegal access to a low address < isdn function decoded>
```

Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.

Workaround: There is no workaround.

Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.

- CSCsw29842

Symptoms: A router may reload or crash at resource_owner_set_user_context while adding and removing MTU in the ATM main interface and subinterface.

Conditions: The symptom is observed when the command **no mtu** on the ATM subinterface modifies the minimum MTU size to zero.

Workaround: Set the MTU size of the subinterface to a default value or the value of the main interface's MTU instead of using **no mtu**.

Further Problem Description: The command **no mtu** on the ATM subinterface will modify the MTU size to zero. It should inherit the default value or value from the main interface if the main interface has an MTU value set. This issue does not affect any functionality of MTU.

- CSCsw30847

Symptoms: The standby router may crash.

Conditions: The symptom is observed when two IMA interfaces are configured on a Cisco 7500 series router along with HA RPR+ mode. When you try to unconfigure the ima-group from the first member of IMA interfaces, the crash will occur.

Workaround: There is no workaround.

- CSCsw31019

Symptoms: A Cisco router crashes.

Conditions: This symptom is observed if the **frame-relay be 1** command is issued under “map-class frame-relay <name>” configuration.

Workaround: There is no workaround.

- CSCsw34224

Symptoms: A router may reload unexpectedly.

Conditions: The symptom is observed when configuring “auto qos/discovery” on the ATM SVC.

Workaround: There is no workaround.

- CSCsw39039

Symptoms: A fax relay call may fail.

Conditions: The symptom is observed with an MGCP Gateway Controlled T38 fax-relay call. MGCP is configured for CA control T38. The output of the command **show call active voice brief** will give the remote address to be 0.0.0.0. When this happens, all fax packets on the ingress gateway are dropped.

Workaround: Use Cisco IOS Release 12.4(15)T7.

- CSCsw39985

Symptoms: Too many IPC error messages are seen.

Conditions: The symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.4 with dLFloLL configuration. The standby router cannot be accessed when the router is HA setup.

Workaround: There is no workaround.

- CSCsw40165

Symptoms: A router may crash.

Conditions: The symptoms are observed when trying to configure the command **translate lat <word> ppp <ip> max-users 4294967295** and check it in the running configuration.

Workaround: There is no workaround.

- CSCsw40248

Symptoms: Service policy disappears after removing and attaching to other class-maps under the same policy-map.

Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.4(23.10)T.

Workaround: There is no workaround.

- CSCsw42244

Symptoms: Traceback may be observed on a Cisco 3845 MGCP gateway.

Conditions: The symptom is observed with a Cisco 3845 MGCP gateway during an SNMP walk.

Workaround: There is no workaround.

Further Problem Description: In order to set isdnBearerOperStatus during an SNMP walk, false-busy out condition of B channel is checked. In order to check the false-busy status for all interfaces, DSL information is extracted from the idb list. The idb list for the particular DSL can be NULL with a bulk SNMP query, and it is not checked for NULL before accessing. In this scenario, isdnBearerOperStatus should have only default value which is D_isdnBearerOperStatus_idle.

- CSCsw43948

Symptoms: A Cisco 3845 router that is running Cisco IOS Release 12.4(13) may bounce the frames (which are not destined for itself) on the same interface that receives them.

Conditions: The symptom is observed if there is bridging configured on an ethernet subinterface in the following way:

```
ip cef
!
bridge irb
!
interface GigabitEthernet0/1
 no ip address
 no sh
!
!
interface GigabitEthernet0/1.100
 encapsulation dot1Q 100
 ip address x.x.x.x x.x.x.x
 no ip redirects
 no ip unreachable
 no ip proxy-arp
 ip rip advertise 10
!
interface GigabitEthernet0/1.509
 encapsulation dot1Q 101
 bridge-group 1
```

Workaround: If the command **bridge-group 1** is removed from the sub-interface, it will behave as expected.

- CSCsw45691

Symptoms: The atmPreviouslyFailedPVCTimeStamp returns a non-zero value when the VC is brought DOWN for the first time.

Conditions: This issue is seen on router that is running Cisco IOS Release 12.4(24)T.

Workaround: There is no workaround.

- CSCsw47543

Symptoms: A router may lose all its free memory and crash.

Conditions: The symptom is observed when the voice mail system sends a notification to the gateway regarding the availability of any voice messages. The memory leaks occurs in CDAPI_RawS.

Workaround: Use the command **signalling forward none** under the global configuration “voice service voip”.

- CSCsw49297

Symptoms: Packet drops and/or delays are observed when sending traffic over a multilink bundle interface.

Conditions: This symptom may occur during periods of bursty traffic.

Workaround: Increase the amount of data that a multilink will queue to a member link at any given time using the interface configuration command **ppp multilink queue depth qos** (default = 2). This command may be configured on the serial interfaces or, if the interface is a multilink group member, it may be configured on the multilink interface. For example:

```
interface Multilink1 ppp multilink queue depth qos 3
```

- CSCsw52416

Symptoms: Dynamic NAT entries are not timing out properly

Conditions: Occurs even after timer expired.

Workaround: There is no workaround.

- CSCsw63356

Symptoms: The following messages may be seen when bringing up a WIC-1DSU-T1-V2:

```
%SERVICE_MODULE-4-WICNOTREADY: (with traceback) and/or
WARNING - timeslots command not accepted by service-module % Service module
configuration command failed: LOCK OBTAIN TIMEOUT.
```

Conditions: The symptom is observed with a Cisco 3825 and a 3845 router where WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present in one or more WIC/HWIC slots and one WIC-1DSU-T1-V2 is in any of the NM slots. In this setup, the problem will be seen on the highest number WIC/HWIC slot where WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present.

Workaround: Use WIC-1DSU-T1-V2 in either WIC slots or NM slots (not in both).

Alternate workaround: Use Cisco IOS Release prior to 12.4(15)T7.

- CSCsw65929

Symptoms: A crash may occur upon disabling ccm-manager fallback.

Conditions: The symptom is observed when disabling and enabling MGCP application and ccm-manager fallback in quick succession.

Workaround: There is no workaround.

- CSCsw66082

Symptoms: A router crash may be seen at ip_mcast_address_lookup when issuing the **show ip igmp ssm-mapping multicast group** on an SSM-mapping enabled router which makes use of DNS lookup for source list.

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS release 12.4(23.10)T.

Workaround: There is no workaround.

- CSCsw66086

Symptoms: A router may crash with a segmentation violation (SegV) exception in MPLS code.

Conditions: The symptom is observed when “ip route-cache flow” is configured on an MPLS interface.

Workaround: There is no workaround.

- CSCsw67040
Symptom: A Cisco 5850 may crash.
Conditions: The symptom is observed on a Cisco 5850 that is running Cisco IOS Release 12.4(23).
Workaround: There is no workaround.
- CSCsw71188
Symptoms: A Cisco 7200 series router may lose connectivity to the SDH link.
Conditions: The symptom is observed under the following conditions:
1. The Cisco 12416 router receives a PAIS Alarm from the Optical Network. 2. The interfaces go down and up and the ALARM is cleared from the Cisco 12416 router side. 3. The Cisco 7200 series router loses connectivity. 4. The Cisco 12416 router interface POS is still UP, but the ping fails. 5. After interface is shutdown and re-enabled, it is in serial UP but protocol DOWN from the Cisco 12416 router side. 6. The link is recovered when the fiber is disconnected and reconnected from the Cisco 7200 series router side.
Workaround: Disconnect and re-connect the fibers from the Cisco 7200 series router side.
- CSCsw76730
Symptoms: PVCs are not in the desired state when the interface is down and, when verifying, the translation entry is deleted.
Conditions: The symptom is observed on a Cisco router when the **show x25 vc 1** command is used. No output is given.
Workaround: There is no workaround.
- CSCsw77293
Symptoms: Upon unconfiguring “channel-group” in one controller, the ping fails in another controller.
Conditions: The symptom is observed when a controller is configured and then unconfigured with “channel-group”.
Workaround: Configure “channel-group” again.
- CSCsw85152
Symptoms: No flows are seen in the protocol-port aggregation cache. Essentially, the feature is not working.
Conditions: The symptom is observed with a Cisco 7200 series router that is running Cisco IOS Release 12.4(24) onwards.
Workaround: There is no workaround.
- CSCsw85235
Symptoms: FTP copy fails, giving the error message “Incorrect Login/Password”.
Conditions: The symptom is observed when copying a file using FTP and using the username and password in the command itself.
Workaround: Set FTP username/password in router using the **ip ftp** command.
- CSCsx06457
Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx09343

Symptoms: PKI daemon is stuck in DNS resolution attempt for the hostname used in the CDP.

Conditions: The symptom is observed when using name resolution for automatic actions taken by the router during non-interactive sessions (CRL download using name in CDP URI). This issue has been seen to occur only on a Cisco Catalyst 6500 running Cisco IOS SXH software.

Workaround: There is no workaround.

- CSCsx11776

Symptoms: Executing the commands **show ip bgp version recent 1** or **show ip bgp version 1** from EXEC mode may cause the device to crash.

Conditions: The symptom is observed in affected images that have support for BGP.

Workaround: Use AAA command authorization to prevent the use of these commands.

Further Problem Description: A note regarding BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers:

BGP Looking Glass servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A Looking Glass server (or LG server) is accessed remotely for the purpose of viewing routing info. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the lg server. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

Public Looking Glass servers running an affected version of Cisco IOS are specially susceptible to this bug because they provide unauthenticated public access to Cisco IOS devices. Because of this, operators of BGP Looking Glass servers are encouraged to use AAA to prevent execution of the commands mentioned above that are known to crash Cisco IOS.

- CSCsx14637

Symptoms: Modem pass-through calls failing while handshaking

Conditions: Problem appeared after upgrade from Cisco IOS Release 12.3(26) Cisco IOS Release to 12.4(23)

Workaround: There is no workaround.

- CSCsx15358

Symptoms: A router may crash after receiving DNS TCP queries.

Conditions: The symptom is observed on a router with “ip dns server” configured.

Workaround: There is no workaround.

- CSCsx15370

Symptoms: EIGRP commands may disappear from the interface configuration.

Conditions: The symptom is observed on Cisco routers that are running Cisco IOS Release 12.4T and following an interface flap.

Workaround: There is no workaround.

- CSCsx19184

Symptoms: Cisco 2821 got bus error crash even though there was no configuration change or hardware change.

Conditions: Happens while running an internal image with potential fix for CSCsv20948 and CSCsw44230.

Workaround: There is no workaround.

- CSCsx23456

Symptoms: The standby reloads on a Cisco 7500 series router.

Conditions: The symptom is observed when IMA PA is configured on a Cisco 7500 series router and where RPR+ is configured. It is seen when an OIR is done on the VIP where IMA PA is sitting.

Workaround: There is no workaround.

- CSCsx23602

Symptoms: Catalyst 6000 running modular Cisco IOS 12.2(33)SXH4 may crash with NAT configuration.

Conditions: Occurs when running modular IOS with NAT deployment. Crash only happening in production, and NAT translation is required for crash to occur.

Workaround: Run non-modular Cisco IOS Release 12.2(33)SXH4.

- CSCsx40747

Symptoms: A specific configuration of “ip casa” followed by a subsequent use of the command **show running-config** can cause the router to go into an infinite loop and hang.

Conditions: The symptom is observed when “ip casa” is configured and you enter into config-casa mode. The command **show running-config** will cause the router to hang.

Workaround: There is no workaround.

Further Problem Description: This issue is specific to the usage of ip casa. If you do not use casa, you are not vulnerable to the issue described here.

- CSCsx47915

Symptoms: Spurious memory access and alignment error observed when removing policy-map from interface under certain configuration sequence.

Conditions: The problem is seen on Cisco routers running Cisco IOS Release 12.4(18e).

Workaround: There is no workaround.

- CSCsx58889

Symptoms: Calls fail intermittently with cause “47: no resource available” error.

Conditions: Occurs when router is under load test.

Workaround: There is no workaround.

- CSCsx59039

Symptoms: Router crashes at SCCP SPI functions when handling events from STCAPP.

Conditions: This is a corner case that occurs rarely. Only if STCAPP unregisters its SCCP device (forced by a DSP problem, in this case) while the corresponding voice-port is still active (having some internal event in the SCCP SPI queue to be processed after the unregistration), the crash can occur.

Workaround: There is no workaround.

- CSCsx59436

Symptoms: Cisco 837 experiences failure of LAN ports after power cycle. If the LAN port is set to 100/Full, the connection to the other device cannot be reestablished.

Conditions: Occurs on a router running either Cisco IOS Release 12.3 or 12.4.

Workaround: Set the LAN port to duplex and speed Auto/Auto.

- CSCsx61885

Symptoms: Cisco AS5850 running an internal image based on Cisco IOS Release 12.4(23) may crash unexpectedly.

Conditions: Occurs during normal operation.

Workaround: There is no workaround.

- CSCsx74657

Symptoms: Multiple issues are seen on multicast NAT. NAT is adding the number of dynamic entry statistics for every new multicast packet, even though there is already an existing NAT flow entry. This causes the number of dynamic entries to be inconsistent with the output from **show ip nat trans**. Also, dynamic NAT entries cannot be deleted with **clear ip nat trans ***. Finally, every fragmented multicast packet creates a separate NAT entry.

Conditions: Occurs when **ip pim sparse-dense-mode** is configured on the interfaces with NAT overload.

Workaround: There is no workaround.

- CSCsx82690

Symptoms: A voice gateway placing ISDN calls will exhibit a memory leak. The effects of this memory leak can be seen with the **show process memory** command. It shows that the amount of memory the ISDN process is holding continues to increase without being released.

Conditions: The symptom is observed on a voice gateway that is processing ISDN calls on a PRI interface. Switchtype is set to be primary-QSIG and the calls that leak memory are QSIG-GF (connection-oriented calls) and not regular voice calls. Such calls are typically used when implementing supplementary services such as MWI.

Workaround: There is no workaround.

- CSCsx83443

Symptoms: ISKMP debug messages from all peers are shown in the terminal monitor enable tty/vty's even though **debug crypto condition peer ipv4 x.x.x.x** is set.

Conditions: Use peer IP-based debug condition.

Workaround: There is no workaround.

- CSCsy14551

Symptoms: Router may experience problem while erasing flash when running Cisco IOS Release 12.4(24.6a).

Conditions: It occurs when changing from high-end to low-end file system, or from low-end to high-end file system.

Workaround: There is no workaround.

- CSCsy14816

Symptoms: Router crashes when configuring **wlccp authentication-server client** after the client has been removed by another user.

Conditions: Occurs after configuring a wlccp authentication-server client and before reconfigure another user in another console removes the same.

- Workaround: There is no workaround.
- CSCsy14973
Symptoms: L2TP Tunnel will not come up.
Conditions: Occurs during normal operation.
Workaround: There is no workaround.
 - CSCsy15098
Symptoms: Cisco 3845 reloads at `cm_destroy_connection` while changing mode ATM AIM 0 to CAS.
Conditions: Occurs while switching a Cisco 3845 with an existing connection.
Workaround: There is no workaround.
 - CSCsy16177
Symptoms: Cisco 2811 experiences invalid checksum over SCP on SSH version 2.
Conditions: Occurs on a Cisco 2811 with flash type file system.
Workaround: There is no workaround.
 - CSCsy16519
Symptoms: “ifDescr” not populated for WS-SVC-CMM.
Conditions: Occurs when performing SNMP walk.
Workaround: There is no workaround.
 - CSCsy20189
Symptoms: In MVPN set up, the **show ip pim rp mapping** command and **show ip rpf** command take a long time to display. the output, and multicast ping not going fine
Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(24.6a).
Workaround: There is no workaround.
 - CSCsy20503
Symptoms: Use of the **summary-prefix<prefix> not-advertise** does not suppress the prefix.
Conditions: Occurs on routers running Cisco IOS Release 12.4(24.1) and beyond.
Workaround: Enter the **clear ipv6 ospf process** command.
 - CSCsy22311
Symptoms: Using secure copy (SCP) between Cisco routers may cause compatibility issues.
Conditions: Occurs when using SCP SSH version 2 between a Cisco 1800 and Cisco 2800.
Workaround: There is no workaround.
 - CSCsy23362
Symptoms: Router crash and traceback seen @PKI_BindSessionTrustPoint while the traffic flow is initiated between test routers after applying the crypto map.
Conditions: Apply the crypto map on the routers and try to ping. At this point the router crashes.
Workaround: There is no workaround.
 - CSCsy23892

Symptoms: A Cisco router may experience a spurious access, a crash, or a hang when doing a **no match class-map** under a class map configuration. The spurious access is the most likely one to be seen.

Conditions: This can occur when the match class-map statement does not exist under the class map.

Workaround: There is no workaround.

- CSCsy29828

Symptoms: A Cisco router may reload due to a bus error. The error indicates trying to read address 0x0b0d0b**, where ** is around 29.

Conditions: This has been experienced on a Cisco 2800 series router running Cisco IOS Release 12.4(24)T. The router must be configured with NAT, and SIP traffic is passed through the NAT router.

Workaround: Enter the following commands:

* **no ip nat service sip tcp port 5060**

* **no ip nat service sip udp port 5060**

Or

* **ip nat translation timeout never**

- CSCsy45371

Symptoms: The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

Conditions: Occurs when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

Workaround: Stop the network traffic while configuring NAT.

- CSCsy97506

Symptoms:

Case 1: All NAT multicast data packets are processed by software.

Case 2: Spurious memory access occurs.

Conditions:

Case 1. NAT with static port entry, or dynamic overload configuration.

Case 2. Configure **ip nat dynamic nat** rule with an undefined NAT pool.

Workaround:

Case 1: Configure NAT as static entry without port, or dynamic non-overload.

Case 2: Configure with defined pool.

- CSCsz02000

Symptoms: Router reloads at “atm_update_bundle_counters”.

Conditions: Occurs during normal operation.

Workaround: There is no workaround.

- CSCsz05783

Symptoms: Voice/SIP (ef) packets are not marking in the ingress/egress when NAT is enabled on the interface.

Conditions: Occurs when NAT is enabled.

Workaround: Remove NAT from the configuration.

Resolved Caveats—Cisco IOS Release 12.4(23b)

Cisco IOS Release 12.4(23b) is a rebuild release for Cisco IOS Release 12.4(23). The caveats in this section are resolved in Cisco IOS Release 12.4(23b) but may be open in previous Cisco IOS releases.

- CSCsk80250

Symptoms: A router may reload.

Conditions: This symptom is observed when the **show ip bgp neighbors x.x.x.x paths** `^([7][0][1][8].l..l.....)+_7018_` command is issued.

Workaround: There is no workaround.

- CSCsw63356

Symptoms: The following messages may be seen when bringing up a WIC-1DSU-T1-V2:

```
%SERVICE_MODULE-4-WICNOTREADY: (with traceback)
```

and/or

```
WARNING - timeslots command not accepted by service-module % Service module  
configuration command failed: LOCK OBTAIN TIMEOUT.
```

Conditions: This symptom is observed with a Cisco 3825 and Cisco 3845 router where a WIC-1DSU-T1-V2 or a HWIC-1DSU-T1 is present in one or more WIC/HWIC slots and one WIC-1DSU-T1-V2 is in any of the NM slots. In this setup, the problem will be seen on the highest number WIC/HWIC slot where the WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present.

Workaround: Use the WIC-1DSU-T1-V2 in either WIC slots or NM slots (but not in both).

Alternate Workaround: Downgrade to an earlier release that does not have the support for HWIC-1DSU-T1.

- CSCsx20984

Symptoms: Router reloads with a bus error and no tracebacks.

Conditions: Unknown at this time.

Workaround: There is no workaround.

- CSCsx25880

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml>.

- CSCsx70889

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsz29815
Symptoms: TTY sessions not accessible after reverse SSH session to the same TTY port results in failed authentication.
Conditions: Occurred on a router running Cisco IOS Release 12.4(24)T and configured with TTY lines accessed using reverse SSH version 2. Issue also affects SSH version 1 and affects VTY lines.
Workaround: Reload the router.
- CSCsz38104
The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml>.
- CSCsz48392
Symptoms: Doing reverse SSH to a TTY line, which is busy, causes the terminal server to crash.
Conditions: This issue is encountered in a Cisco 3845 router that is running Cisco IOS Release 12.4(23).
Workaround: There is no workaround.
- CSCsz50423
Symptoms: The **clear interface atm5/ima** command makes the ATM PVC inactive.
Conditions: This symptom occurs on a Cisco 7200 router that is running Cisco IOS interim Release 12.4(24.6)T8.
Workaround: There is no workaround.
- CSCsz56169
Symptoms: A software-forced crash occurs after a **show user** command is performed.
Conditions: The crash occurs after the user performs a **show user** command and then presses the key for next page. It is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(21a).
Workaround: Do not perform a **show user** command.
- CSCta77552
Symptoms: A Cisco 5850 crashed 2 minutes after card in slot 5 crashed.
Conditions: This symptom was observed on a Cisco 5850 with Cisco IOS Release 12.4(25).
Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(23a)

Cisco IOS Release 12.4(23a) is a rebuild release for Cisco IOS Release 12.4(23). The caveats in this section are resolved in Cisco IOS Release 12.4(23a) but may be open in previous Cisco IOS releases.

- CSCsc78999
Symptoms: An Address Error exception occurs after Uninitialized timer in TPLUS process.
Conditions: This is a platform independent (AAA) issue. It may be seen with a large number of sessions while accounting is configured with a T+ server.

Workaround: Disable accounting, or use RADIUS accounting instead of a T+ server.

- CSCsi17158

Symptoms: Devices running Cisco IOS may reload with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

Conditions: This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

Workaround: There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with “ssh” removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

More information on configuring ACLs can be found on the Cisco public website:

<http://www.cisco.com/warp/public/707/confaccesslists.html>

- CSCsi25562

Symptoms: Cisco 2600XM router runs out of memory while trying to boot large images.

Conditions: This defect produces crashes under two scenarios:

- 1.) During loading of large images, such as a c2600-adventerprisek9-mz.
- 2.) During reload where router goes into ROMMon.

Workaround: There is no workaround.

- CSCsj36133

Symptoms: A BGP neighbor may send a notification reporting that it received an invalid BGP message with a length of 4097 or 4098 bytes.

Conditions: The problem can be seen for pure IPv4 BGP sessions (no MP-BGP in use) when the router that is running the affected software generates a large number of withdraws in a short time period and fills an entire BGP update message (up to 4096 bytes normally) completely with withdraws. Because of a counting error, the router that is running the affected software can generate an update message that is 1 or 2 bytes too large when formatting withdraws close to the 4096 size boundary.

Workaround: The issue is not seen when multiple address families are being exchanged between BGP neighbors.

- CSCsm97220

Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at the following link

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>

- CSCso87348

Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. Additionally, this single defect can affect T train platforms on limited releases as detailed below.

Conditions: Occurs when NetFlow is configured on one of the following:

- Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
- Catalyst 6500 running Cisco IOS Release 12.2SXH.

Workaround: Disable NetFlow. This is done with the following commands:

- **no ip flow ingress**
- **no ip flow egress**
- **no ip route-cache flow**

Enter the appropriate command for each subinterface for which NetFlow is currently configured.

Other Notes: 12.4(23) is affected by this ddts. The fix is in releases thereafter for 12.4.

The 12.2SRC and 12.2SXH code trains are affected. The specific versions affected are

- 12.2(33)SXH
- 12.2(33)SXH1
- 12.2(33)SXH2
- 12.2(33)SXH2a
- 12.2(33)SRC
- 12.2(33)SRC1

The issue is fixed in the two affected code trains from the 12.2SXH3 and 12.2SRC2 releases onwards. However, for the SXH train, Cisco would recommend the use of SXH4 due to ddts CSCso71955

The following release trains do not have this issue; 12.2(18)SXF, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXI and all other release trains after those affected.

- CSCso90058

Symptoms: MSFC crashes with Red Zone memory corruption.

Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

Workaround: There is no workaround.

- CSCsr18173

Symptoms: 1. If dampening is enabled on a router, and identical updates of a IPv4 prefix carrying label information are received, these updates are not treated as identical and dampening penalty is set for the route. 2. If dampening is enabled on a router, and identical updates of a IPv4 multicast prefix are received, these updates are not treated as identical and dampening penalty is set for the route.

Conditions: The symptom is observed when dampening is enabled and: 1. Identical updates of a IPv4 prefix are received. The updates should be carrying MPLS Label information; or 2. Identical updates of a IPv4-multicast prefix are received.

Workaround: There is no workaround.

- CSCsr59242

Symptoms: EIGRP may lose some routes from stub neighbors in a DMVPN setup.

Conditions: If EIGRP graceful restart happens on an interface and the interface update queue is busy, then it may lose some routes from the stub neighbors on that interface.

For example, issuing the below commands can trigger this issue:

clear ip eigrp vrf abc as-number neighbors interface Wait 30 seconds **clear ip eigrp vrf abc as-number neighbors interface soft**

Workaround: Use the **clear ip eigrp vrf abc neighbors** command to fix the problem.

Another workaround is that graceful restart can be turned off by the **no eigrp graceful-restart** command under the router or the **address-family** command. This will cause the symptom to go away but will revert back to hard resetting peers on configuration changes or the **clear ip eigrp neighbor soft** command.

- CSCsr61125

Symptoms: A switchover takes more time on a Cisco 7500 router.

Conditions: This symptom is observed when RPR+ is configured on the Cisco 7500.

Workaround: There is no workaround.

- CSCsr80601

Symptoms: An ISAKMP SA is not deleted as expected after removing the RSA key.

Conditions: The issue is seen when the user tries to clear the ISAKMP SAs by issuing the **clear crypto session** command on an IKE SA that has multiple IPSEC SAs.

Workaround: Use the **clear crypto sa** and **clear crypto is** commands.

- CSCsu04446

Symptoms: A Cisco router that is running a PfR Master Controller crashes under stress.

Conditions: This symptom is observed when traffic with more than 2000 prefixes with about 500 unreachable prefixes is flowing through the router.

Workaround: Minimize the number of prefixes learned during an interval. The default of 100 should be sufficient.

oer master learn prefixes 100

- CSCsu10229

Symptoms: cdpCacheAddress(OID:1.3.6.1.4.1.9.9.23.1.2.1.1.4) MIB is not showing GLOBAL_UNICAST address.

Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T7.

Workaround: There is no workaround.

- CSCsu25833

Symptoms: An ISR router may crash with the following error message: %ALIGN-1-FATAL: Corrupted program counter

Conditions: The symptoms are observed on a Cisco 2811 and 2801 router. The trigger has not yet been identified.

Workaround: There is no workaround.

- CSCsu26174

Symptoms: A Cisco 1800 series router may stop passing traffic on FastEthernet interface 0/1 when FastEthernet interface 0/0 is administratively shut down using the interface configuration command **shutdown**. When FastEthernet 0/0 is shutdown, the following message is displayed:

```
%GT96K_FE-5-LATECOLL: Late Collision on int FastEthernet0/0
```

Conditions: The symptoms are observed with FastEthernet 0/0 on a Cisco 1841 router and when the device at the far end of interface FastEthernet 0/0 is configured manually to speed 10 or 100.

Workaround: Configure the far-end device to auto-negotiate the speed with the 1800 router.

Further Problem Description: This problem does not occur when pulling out cable and re-inserting in FastEthernet 0/0. It also does not occur when FastEthernet 0/1 is reversed to FastEthernet 0/0.

- CSCsu27888

Symptoms: IGMP v3 reports are discarded.

Conditions: Occurs on Cisco 7200 router running Cisco IOS Release 12.4(20)T2.

Workaround: There is no workaround.

- CSCsu35597

Symptoms: Renaming a directory gives error message.

Conditions: This happens on a Cisco router running Cisco IOS Release 12.4(20)T1.fc2 image

Workaround: There is no workaround.

- CSCsu36836

Symptoms: TCL scripts and policies attempting to work with open files and sockets simultaneously may not operate properly. One symptom is the **vwait** command may fail by reporting “would wait forever”.

Conditions: Occurs when a TCL script opens both a file and a client or server socket simultaneously.

Workaround: Open and close files and sockets separately. Avoid having them open simultaneously.

- CSCsu44789

Symptoms: Spurious memory access traceback is seen.

Conditions: The symptom is observed when an MGCP Gateway tries to defer a Request Notification (RQNT) without the requested/signal event.

Workaround: There is no workaround.

- CSCsu45425

Symptoms: Label Forwarding Information Base (LFIB) shows incorrect information for Global BGP prefix after route flap. LFIB/FIB shows prefix as having a tag when it should be not. Routing table is correct.

Conditions: Occurred on a Cisco 12000 router running Cisco IOS Release 12.0(33)S1.

Workaround: Enter the **clear ip route** command.

- CSCsu48898

Symptoms: A Cisco 10000 series router may crash every several minutes.

Conditions: The symptom is observed with a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB13.

Workaround: Use Cisco IOS Release 12.2(31)SB11.

- CSCsu74397

Symptoms: When removing PA-MC-8TE1+ from the chassis, the router has an unexpected system reload. This reload happens when you remove the port adapter and the router is running the Cisco IOS bootloader image. Also happens when the port adapter is removed after the router finishes loading the Cisco IOS bootloader image and before it loads the complete Cisco IOS Software image.

Conditions: This occurs on a Cisco 7200 VXR NPE-G2 Series Routers on the Cisco IOS bootloader image from the Cisco IOS Release 12.4(4)XD.

Workaround: Remove PA-MC-8TE1+ when the complete Cisco IOS Software Image finishes loading.

- CSCsu92432

Symptoms: The router's async line used for reverse SSHv2 might hang after a failed authentication and not recover unless the router is rebooted. The router log displays:

```
%SYS-3-HARIKARI: Process SSH Process top-level routine exited
```

Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4 with async lines.

Workaround: Use the traditional way of using reverse SSH with the use of rotaries.

- CSCsv01474

Symptoms: The **ip rip advertise** command might be lost from the interface.

Conditions: This symptom occurs in any of the following three cases:

1. The interface flaps. 2. The **clear ip route** command is issued. 3. The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

Workaround: Configure the **timers basic** command under the address-family under rip.

- CSCsv03300

Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard gigabitethernet interface.

Workaround: There is no workaround.

- CSCsv04836

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- CSCsv06608

Symptoms: SXP is set up between two devices but fails to initialize.

Conditions: This symptom is observed when SXP is set up between two devices.

Workaround: There is no workaround.

- CSCsv15266

Symptoms: A router that is running Cisco IOS Release 12.4 with QoS configured with a parent and child policy may experience a reset due to a software-forced crash displaying one of the following messages:

```
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
dealloc XXXXXXXX
OR
```

```
%SYS-6-BLKINFO: Corrupted magic value in in-use block blk XXXXXXXX, words XX, alloc
XXXXXXXX, Free, dealloc XXXXXXXX, rfcnt X
```

Conditions: The reset is triggered by a configuration change tied to QoS and has been seen while changing one of the following:

- An access-list referenced by the map-class.
- The DSCP/Precedence values being set by the service-policy.
- Removing the service-policy from the interface.
- Altering the shaping parameters within the service-policy.

Workaround: Other than avoid making changes to the QoS outside of a maintenance window, there is no workaround.

- CSCsv20948

Symptoms: The primary router may crash continually.

Conditions: The symptom is observed with two Cisco 3825 routers with the same software and hardware and with a situation where one is working as a primary router and the other as a secondary. The issue is seen only with voice traffic. It is observed when running Cisco IOS Release 12.4(20)T (with this release the primary router crashes very frequently) and also with Cisco IOS Release 12.4(20)T1.

Workaround: There is no workaround.

- CSCsv27607

Symptoms: BGP router filters outbound routes to the peers when doing soft reset with specifying peer address using the **clear ip bgp ip-addr soft out** command. However, the routes to be filtered are not deleted from the routing table on the BGP peer router.

Conditions: The symptom happens when removing and then reapplying an outbound route-map. When issuing the **clear ip bgp neighbor-address soft out** command for each peer in an update-group after applying the outbound route-map filtering policy. The withdraw for filtered prefixes is sent to the first peer specified in soft reset, but the next peers in the same update-group do not withdraw the routes.

Workaround: Perform a hard BGP reset using the **clear ip bgp ip-addr** command.

- CSCsv28806

Symptoms: When a dspfarm profile still has active calls, if the user manually shuts down the dspfarm profile, the router will crash.

Conditions: The user manually shuts down a dspfarm profile when it is still in use with active calls. This includes the case where a dspfarm profile is manually shut down after a DSP crash occurs to the dspfarm service but the endpoint phones have not yet finished hanging up.

Workaround: Do not shut down a dspfarm profile if it is still in use by active calls. Besides, if a DSP crash occurs, hang up all the phones using that dspfarm service and wait until the DSP sessions are released before manually shutting down the dspfarm profile.

- CSCsv38166

The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>.

- CSCsv40404

Symptoms: When DDNS is disabled on the router which is configured as the DHCP server, it sends option 81 in the DHCP ACK message with the N flag bit set to 1. However, the DHCP client fails to understand this and will not undertake a PTR update.

Conditions: The issue is seen with a third-party vendor DNS server and a Cisco IOS DHCP server.

Workaround: There is no workaround.

Further Problem Description: The issue is not seen with the 12.3 code as it does not support DDNS and hence does not reply back with Option 81 in the DHCP ACK.

- CSCsv42636

Symptoms: A Cisco 1721 reloads due to a bus error.

Conditions: The symptom is observed on a Cisco 1721 which is configured for AAA and is running Cisco IOS Release 12.4(16a), 12.4(16b) and 12.4(21). This is a platform independent issue and can possibly be seen on other platforms.

Workaround: There is no workaround.

- CSCsv52459

Symptoms: A Cisco device that is running Cisco IOS Release 12.3(7)T or later Cisco IOS code may see an increase in CPU usage when upgrading from a previous image.

Conditions: NAT must be enabled for the contributing factor described here to be applicable. RTSP and MGCP NAT ALG support was added, which requires NBAR. However, there is no way to disable it if that feature code is not needed.

Workaround: There is no workaround.

- CSCsv54130

Symptoms: Ping fails in HWIC-2T and WIC-2T when the physical mode is changed to “Async” from “Sync” with PPP encapsulation.

Conditions: The symptom is observed when the initial configuration is in Sync mode as shown:

```
interface Serial0/1/0
ip address x.x.x.x 255.0.0.0
encapsulation ppp
end
```

Then the configuration is changed to Async mode:

```
Current configuration: 123 bytes
interface Serial0/1/0
physical-layer async
ip address x.x.x.x 255.0.0.0
encapsulation slip
async mode dedicated
end
```

Workaround: Toggling the encapsulation to PPP sometimes fixes the issue. This may have to be done multiple times until the interface comes up.

- CSCsv59334

Symptoms: Upon entering the configuration command **no network 0.0.0.0 0.0.0.0** under the eigrp router configuration mode, all the EIGRP routes that were redistributed get withdrawn.

Conditions: The symptom is observed when using explicit network prefixes as well as network 0.0.0.0/32 which includes unspecified, directly connected networks to enable EIGRP on various interfaces of a router. These EIGRP routes are also redistributed into BGP. In such a case, on entering the configuration command **no network 0.0.0.0 0.0.0.0** under the eigrp router configuration mode, all the EIGRP routes that were redistributed get withdrawn. For example:

```
router eigrp 1
```

```
network 10.0.0.0
```

```
network 0.0.0.0
```

```
Rt130#sh ip eigrp topo
```

```
EIGRP-IPv4 Topology Table for AS(1)/ID(10.1.1.1)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s - sia Status
```

```
P 10.1.1.1/32, 1 successors, FD is 128256
```

```
via Connected, Loopback1
```

```
P 10.1.1.0/24, 1 successors, FD is 281600
```

```
via Connected, Ethernet1/0
```

```
P 10.147.204.64/26, 1 successors, FD is 281600
```

```
via Connected, Ethernet0/2 P 10.147.204.0/26, 1 successors, FD is 281600
```

```
via Connected, Ethernet0/0
```

In the above configuration, network 10.0.0.0/24 is explicitly included under EIGRP by the network 10.0.0.0 configuration. The other networks (13, 20 etc) are included by the network 0.0.0.0 configuration. If EIGRP routes are redistributed into BGP, the three networks 10, 13 and 20 can be seen by BGP. On doing a **no network 0.0.0.0 0.0.0.0**, we would expect the redistribution of networks 13 and 20 to stop while network 10 continues to get redistributed. However, all the networks 10, 13 as well as 20 do not get redistributed into BGP.

Workaround: Clear the IP route and reload to allow the networks to get in the BGP table.

- CSCsv66827

Symptoms: Clearing the SSH sessions from a VTY session may cause the router to crash.

Conditions: The symptom is observed when a Cisco 7300 series router is configured for SSH and then an SSH session is connected. If the SSH session is cleared every two seconds using a script, the symptom is observed.

Workaround: There is no workaround.

- CSCsv73509

Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

Conditions: Configure “no aaa new-model”, configure login local under line vty 0 4 and configure login tacacs under line vty 0 4.

Workaround: There is no workaround.

- CSCsv77932

Symptoms: Router crashes.

Conditions: Occurs while configuring serial interface for insufficient MTU.

Workaround: There is no workaround.

- CSCsv79584

Symptoms: An 0.0.0.0 binding with a 0 minute lease gets created and subsequently removed on the DHCP unnumbered relay.

Conditions: The DHCP client sends a DHCPINFORM with ciaddr set to its address, but giaddr is empty. The relay fills in giaddr with its IP address and the server replies to giaddr. Since the DHCPACK is in response to DHCPINFORM, the lease-time option is absent. Relay receives the DHCPACK and tries to process it normally leading to the route addition.

Workaround: There is no workaround.

Further Problem Description: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP requests. Examining “debug ip routing” for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv87146

Symptoms: Clearing of NAT translation either manually or automatically through timeout results in crash.

Conditions: Occurs when a dynamic translation mapping is removed while traffic is running.

Workaround: Stop traffic before removing dynamic NAT translation.

- CSCsv94099

Symptoms: Traceback may be seen in relay.

Conditions: The symptom is observed in an unnumbered scenario when the client releases the address.

Workaround: There is no workaround.

- CSCsw18636

Symptom:

High CPU utilization after receives a ARP packet with protocol type as 0x1000.

Conditions: This problem occurs on SUP32 running 12.2(33)SXI. This problem may also occur on SUP720. The problem is only seen when you have bridge-group CLI being used which lead to arp pkts with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

Workaround: Filter the ARP packet. The device Config should have bridge-group creation first; followed by interface specific bridge-group options.

Additional-Info.

This problem is now isolated to command ordering in the startup-config file. bridge <> command is saved before bridge-group <> command (which is run in the interface-config mode) is saved. The linking of IDB to bridge structure is not happening correctly and some check fails in the bridge code that lets the packet to be processed again and again instead of being dropped.

If bridge-group <> command is removed in the startup-config and only applied after bridge <> command is run, problem will go away. Please use this workaround until a fix is put in.

- CSCsw23397

Symptoms: A Cisco Communication Media Module (CMM) may leak memory in the chunk manager.

Conditions: The symptom appears to be triggered by calls that disconnect prematurely.

Workaround: There is no workaround.

Further Problem Description: Though this problem is seen and reported on CMM, it may occur on any IOS gateway supporting voice (28xx, 38xx, 5xxx).

- CSCsw24542

Symptoms: A router may crash due to a bus error after displaying the following error messages:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error, %ALIGN-1-FATAL: Illegal access to a low address < isdn function decoded>
```

Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.

Workaround: There is no workaround.

Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.

- CSCsw24700

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253. 2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities.

There are no workarounds that mitigate these vulnerabilities.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

- CSCsw39039

Symptoms: A fax relay call may fail.

Conditions: The symptom is observed with an MGCP Gateway Controlled T38 fax-relay call. MGCP is configured for CA control T38. The output of the command **show call active voice brief** will give the remote address to be 0.0.0.0. When this happens, all fax packets on the ingress gateway are dropped.

Workaround: Use Cisco IOS Release 12.4(15)T7.

- CSCsw49297

Symptoms: Packet drops and/or delays are observed when sending traffic over a multilink bundle interface.

Conditions: This symptom may occur during periods of bursty traffic.

Workaround: Increase the amount of data that a multilink will queue to a member link at any given time using the interface configuration command **ppp multilink queue depth qos** (default = 2). This command may be configured on the serial interfaces or, if the interface is a multilink group member, it may be configured on the multilink interface. For example:

```
interface Multilink1 ppp multilink queue depth qos 3
```

- CSCsw52416

Symptoms: Dynamic NAT entries are not timing out properly

Conditions: Occurs even after timer expired.

Workaround: There is no workaround.

- CSCsw66082

Symptoms: A router crash may be seen at ip_mcast_address_lookup when issuing the **show ip igmp ssm-mapping multicast group** on an SSM-mapping enabled router which makes use of DNS lookup for source list.

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS release 12.4(23.10)T.

Workaround: There is no workaround.

- CSCsw67040

Symptom: A Cisco 5850 may crash.

Conditions: The symptom is observed on a Cisco 5850 that is running Cisco IOS Release 12.4(23).

Workaround: There is no workaround.

- CSCsw71188

Symptoms: A Cisco 7200 series router may lose connectivity to the SDH link.

Conditions: The symptom is observed under the following conditions:

1. The Cisco 12416 router receives a PAIS Alarm from the Optical Network.
2. The interfaces go down and up and the ALARM is cleared from the Cisco 12416 router side.
3. The Cisco 7200 series router loses connectivity.
4. The Cisco 12416 router interface POS is still UP, but the ping fails.
5. After interface is shutdown and re-enabled, it is in serial UP but protocol DOWN from the Cisco 12416 router side.
6. The link is recovered when the fiber is disconnected and reconnected from the Cisco 7200 series router side.

Workaround: Disconnect and re-connect the fibers from the Cisco 7200 series router side.

- CSCsx06457

Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx11776

Symptoms: Executing the commands **show ip bgp version recent 1** or **show ip bgp version 1** from EXEC mode may cause the device to crash.

Conditions: The symptom is observed in affected images that have support for BGP.

Workaround: Use AAA command authorization to prevent the use of these commands.

Further Problem Description: A note regarding BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers:

BGP Looking Glass servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A Looking Glass server (or LG server) is accessed remotely for the purpose of viewing routing info. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the lg server. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

Public Looking Glass servers running an affected version of Cisco IOS are specially susceptible to this bug because they provide unauthenticated public access to Cisco IOS devices. Because of this, operators of BGP Looking Glass servers are encouraged to use AAA to prevent execution of the commands mentioned above that are known to crash Cisco IOS.

- CSCsx14637

Symptoms: Modem pass-through calls failing while handshaking

Conditions: Problem appeared after upgrade from Cisco IOS Release 12.3(26) Cisco IOS Release to 12.4(23)

Workaround: There is no workaround.

- CSCsx19184

Symptoms: Router crash due to Address Error:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xFFFFFFFF

Conditions: This has been seen on Cisco routers running 12.4T and 12.4 images with SIP traffic.

Workaround: There is no workaround.

- CSCsx23602

Symptoms: Catalyst 6000 running modular Cisco IOS 12.2(33)SXH4 may crash with NAT configuration.

Conditions: Occurs when running modular IOS with NAT deployment. Crash only happening in production, and NAT translation is required for crash to occur.

Workaround: Run non-modular Cisco IOS Release 12.2(33)SXH4.

- CSCsx58889

Symptoms: Calls fail intermittently with cause "47: no resource available" error.

Conditions: Occurs when router is under load test.

Workaround: There is no workaround.

- CSCsx61885

Symptoms: Cisco AS5850 running an internal image based on Cisco IOS Release 12.4(23) may crash unexpectedly.

Conditions: Occurs during normal operation.

Workaround: There is no workaround.

- CSCsx74657

Symptoms: Multiple issues are seen on multicast NAT. NAT is adding the number of dynamic entry statistics for every new multicast packet, even though there is already an existing NAT flow entry. This causes the number of dynamic entries to be inconsistent with the output from **show ip nat trans**. Also, dynamic NAT entries cannot be deleted with **clear ip nat trans ***. Finally, every fragmented multicast packet creates a separate NAT entry.

Conditions: Occurs when **ip pim sparse-dense-mode** is configured on the interfaces with NAT overload.

Workaround: There is no workaround.

- CSCsy15227

Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

- CSCsy16177

Symptoms: Cisco 2811 experiences invalid checksum over SCP on SSH version 2.

Conditions: Occurs on a Cisco 2811 with flash type file system.

Workaround: There is no workaround.

- CSCsy22311

Symptoms: Using secure copy (SCP) between Cisco routers may cause compatibility issues.

Conditions: Occurs when using SCP SSH version 2 between a Cisco 1800 and Cisco 2800.

Workaround: There is no workaround.

- CSCsy29828

Symptoms: A Cisco router may reload due to a bus error. The error indicates trying to read address 0x0b0d0b**, where ** is around 29.

Conditions: This has been experienced on a Cisco 2800 series router running Cisco IOS Release 12.4(24)T. The router must be configured with NAT, and SIP traffic is passed through the NAT router.

Workaround: Enter the following commands:

* **no ip nat service sip tcp port 5060**

* **no ip nat service sip udp port 5060**

Or

* **ip nat translation timeout never**

- CSCsy45371

Symptoms: The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

Conditions: Occurs when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

Workaround: Stop the network traffic while configuring NAT.
- CSCsy97506

Symptoms:

Case 1: All NAT multicast data packets are processed by software.

Case 2. Spurious memory access occurs.

Conditions:

Case 1. NAT with static port entry, or dynamic overload configuration.

Case 2. Configure **ip nat dynamic nat** rule with an undefined NAT pool.

Workaround:

Case 1: Configure NAT as static entry without port, or dynamic non-overload.

Case 2: Configure with defined pool.
- CSCsz02000

Symptoms: Router reloads at “atm_update_bundle_counters”.

Conditions: Occurs during normal operation.

Workaround: There is no workaround.
- CSCsz05783

Symptoms: Voice/SIP (ef) packets are not marking in the ingress/egress when NAT is enabled on the interface.

Conditions: Occurs when NAT is enabled.

Workaround: Remove NAT from the configuration.
- CSCsz70666

Symptoms: The **show version** command shows the reload reason as “power-on”.

Conditions: Occurs on a Cisco AS5850 configured for HOS mode when it is rebooted with a time lag.

Workaround: There is no workaround.
- CSCsz87499

Symptoms: Memory leaks occur for SIP calls in a SIP gateway.

Conditions: Occurs with regular SIP calls from PSTN through SIP voice gateway.

Workaround: There is no workaround.
- CSCsz87529

Symptoms: Gateway crashes due to lack of memory.

Conditions: Memory leak occurs in RTCP while processing calls. Due to lack of memory, the gateway crashes.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(23)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(23). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(23). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCek32744

Symptoms: The VLAN-ID is not propagated in the NAS Port ID field when the PPPoE over VLAN call is up.

Conditions: The symptom is observed when using both configurations (main interface and sub-interface) for PPPoE over VLAN. The NAS Port ID value shows correctly while using the sub-interface configuration but incorrectly when using the main interface. The main interface used for PPPoE over VLAN is shown below:

```
interface Ethernet1/0
  no ip address
  vlan-id dot1q 4
  pppoe enable group global
  exit-vlan-config
```

The expected NAS Port ID is 1/0/0/4 but 1/0/0/0 is received.

Workaround: There is no workaround.

Further Problem Description: This will impact AAA as this information should be updated by PPP to AAA.

- CSCek34097

Symptoms: The router may display CPUHOG errors and/or reload when you enter the **no ipv6 multicast-routing** global configuration command.

Conditions: This symptom is observed with configurations that include large numbers of dot1q subinterfaces.

Workaround: There is no workaround.

- CSCek64863

Symptoms: DHCP Relay crashes while sending a DHCP offer to the client with binding as relay binding. (0.0.0.0).

Conditions:

1. Client is either not sending the client-id option or sending the MAC address as the client-id option in all the DHCP messages toward DHCP Relay.
2. Either smart relay is configured on the relay or relay is unnumbered so that relay bindings get created on the router.

Workaround: Disable smart-relay functionality if enabled. Use numbered relay instead of unnumbered relay.

- CSCek71050

Symptoms: Compared to other Cisco IOS software releases, unusually high CPU usage may occur in the BGP router process on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

Conditions: This symptom is observed when BGP is learning routes from the RIB, even if redistribution is not directly configured under BGP. (Redistribution from other routing protocols to BGP can exacerbate the CPU usage.)

Workaround: There is no workaround.

- CSCek77424

Symptoms: A Cisco router that is running Cisco IOS Release 12.4(13b) might unexpectedly reload with a bus error.

Conditions: This symptom happens during normal operation with NAT configured.

Workaround: There is no workaround.

- CSCsb63652

Symptoms: BGP convergence is very slow, and CPU utilization at the BGP Router process is always near 100 percent during the convergence at the aggregation router. This issue obviously shows the following tendencies:

1. The greater the number of component prefixes that belong to the aggregate- address entry, significantly slower convergence is seen at the aggregation router.
2. The greater the number of duplicate aggregation component prefixes for the aggregate-address entry, seriously slower convergence is seen at the aggregation router.

Conditions: Any release would be affected if “aggregate-address” is configured and routing updates are received every few seconds.

Workaround: Remove the “aggregate-address”.

Further Problem Description: If you configure “aggregate-address” lines after BGP convergence has been achieved, the BGP process only holds about 60 or 80 percent of the CPU for about 1 minute. However, if you do peer reset after “aggregate-address” entries have been configured, the convergence time is about 32 minutes (it is about 6 minutes if “aggregate-address” entries are removed).

- CSCsb98906

Symptoms: A memory leak may occur in the “BGP Router” process.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

Workaround: Disable the **bgp regexp deterministic** command.

- CSCsd09324

Symptoms: When reloading a router (lsnt-ap-pe1, Cisco 7500 platform) with Cisco IOS interim Release 12.0(31.4)S1 from any Cisco IOS Release 12.0(28)S4b image, several IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP and traceback occur in the standby log.

Conditions: This symptom has been observed on a Cisco 7500 router platform with MVPN.

Workaround: There is no workaround.

- CSCse26506

Symptoms: When you perform an OIR of an ATM line card, a CPUHOG condition may occur in the “BGP Event” process.

Conditions: This symptom is observed when the ATM line card is configured with about 15,000 /32 routes.

Workaround: There is no workaround.

Further Problem Description: The ATM line card connects to about 15,000 different gateways, each of which is covered by its own /32 route. In addition, there is a less specific route that covers everything. The symptom occurs when BGP attempts to remove a large number of these tracked entries without suspending any.

- CSCsg00102

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCsg39295

Symptoms: Password information may be displayed in a syslog message as follows:

```
%SYS-5-CONFIG-I: Configured from scp://userid:password@10.1.1.1/config.txt by console
```

Conditions: This symptom is observed when using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB; selection of ConfigCopyProtocol of SCP or FTP may result in the password being exposed in a syslog message.

Workaround: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, use the ConfigCopyProtocol of RCP to avoid exposure of the password.

- CSCsg44748

Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW (CUBE) functionality may crash.

Conditions: A gateway configured for IPIPGW functionality with the command **allow-connections** under **voice service voip** under rare conditions will crash while processing VoIP calls.

This has been found to occur in some scenarios where a single VoIP call loops (meaning the call is from the IPIPGW back to the same IPIPGW) through the IPIPGW.

When this occurs, the following error message may be noticed:

```
%SYS-6-STACKLOW: Stack for level Network interfaces running low, 0/9000
```

Workaround:

The workaround is to track down the source of the call looping and correct the problem there.

The other possible workaround is to introduce another termination point in the RTP packet flow beside the IPIPGW. For example, if interworking with Cisco Unified Communications Manager (CallManager) a MTP resource may be used to prevent this loop.

- CSCsg85137

Symptoms: A router that has a Cisco IOS firewall enabled may crash because of a breakpoint exception after the following error message has been generated:

```
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 66596A90.
```

```
-Process= "IP VFR proc and %SYS-2-BADSHARE: Bad refcount in pak_enqueue
```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) or Release 12.4.(12) when the **ip virtual-reassembly** command is enabled on an interface.

Workaround: Disable the virtual fragment reassembly (VFR) configuration on the interface by entering the **no ip virtual- reassembly** command.

- CSCsg90726

Symptoms: Not all the Netmeeting sessions (h323) are obtained in the firewall when enabling the h323 protocol inspection.

Conditions: This is observed when inspection is done with double ACL configured.

Workaround: This workaround applies to the following versions of Netmeeting:

- Microsoft NetMeeting 2.11
- Microsoft NetMeeting 2.1 Standard Edition
- Microsoft NetMeeting 2.11
- Microsoft NetMeeting 2.1 Standard Edition
- Microsoft NetMeeting 3.01 Standard Edition
- Microsoft NetMeeting 2.11
- Microsoft NetMeeting 2.1 Standard Edition
- Microsoft NetMeeting 2.0 Standard Edition
- Microsoft Windows 98 Standard Edition
- Microsoft Windows 98 Second Edition
- Microsoft NetMeeting 3.01 Standard Edition
- Microsoft NetMeeting 3.01 Standard Edition
- Microsoft NetMeeting 3.01 Standard Edition

(<http://support.microsoft.com/kb/158623#appliesto>)

NetMeeting uses the following IP ports to communicate with other meeting participants:

Port	Purpose

389	Internet Locator Server [Transmission Control Protocol (TCP)]
522	User Location Server (TCP)
1503	T.120 (TCP)
1720	H.323 call setup (TCP)
1731	Audio call control (TCP)
Dynamic	H.323 call control (TCP)
Dynamic	H.323 streaming [Realtime Transport Protocol (RTP) over User Datagram Protocol (UDP)]

To enable NetMeeting traffic, you must open a pinhole for these fixed TCP ports also with h323 inspection on the interface.

So the workaround for this is:

1. create the port-map as:

```
ip port-map user-NMAUX port tcp 522 1731 1503 description "Port-map configuration for NetMeeting"
```

2. configure inspection rule as:

```
ip inspect name test h323
```

```
ip inspect name test user-NMAUX
```

```
ip inspect name test ldap
```

(Here Lightweight Directory Access Protocol (LDAP) is included for port 389.)

3. Apply this inspection rule 'test' on the interface where NetMeeting inspection is required.

Example configuration:

```
fwodc1-2#sh run
Building configuration...

Current configuration : 2700 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname fwodc1-2
!
boot-start-marker
boot-end-marker
!
no logging console
enable password lab
!
no aaa new-model
!
!
ip cef
!
!
no ip domain lookup
ip inspect name test tcp
ip inspect name test udp
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
frame-relay switching
!
voice-card 0
  no dspfarm
!
!
!
!
!
```

```

!
!
!
!
!
!
!
!
!
no crypto engine onboard 0
!
!
!
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key letmein address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set test esp-des
!
crypto map test 10 ipsec-isakmp
  set peer 10.0.0.1
  set transform-set test
  match address ipsec_acl
!
!
!
!
interface GigabitEthernet0/1
  ip address 192.168.101.2 255.255.255.0
  ip access-group 102 in
  ip virtual-reassembly
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  encapsulation frame-relay
  clock rate 128000
  no frame-relay inverse-arp

```

```

frame-relay intf-type dce
!
interface Serial0/0/1:587 point-to-point
 ip address 10.0.0.2 255.0.0.0
 ip access-group 101 out
 ip inspect test in
 ip virtual-reassembly
 snmp trap link-status
 frame-relay interface-dlci 587
 crypto map test
!
router eigrp 100
 network 10.0.0.0
 network 192.168.101.0
 no auto-summary
 no eigrp log-neighbor-changes
 no eigrp log-neighbor-warnings
!
 ip forward-protocol nd
!
!
 ip http server
 no ip http secure-server
!
 ip access-list extended ipsec_acl
  permit ip 192.168.101.0 0.0.0.255 192.168.1.0 0.0.0.255
!
 access-list 101 permit udp any any eq isakmp
 access-list 101 permit esp any any
 access-list 101 permit ahp any any
 access-list 101 permit icmp any any
 access-list 101 permit eigrp any any
 access-list 101 deny ip any any
 access-list 102 permit udp any any eq isakmp
 access-list 102 permit esp any any
 access-list 102 permit ahp any any
 access-list 102 permit icmp any any
 access-list 102 permit eigrp any any
 access-list 102 deny ip any any
 access-list 110 permit tcp any any fragments
 access-list 110 permit udp any any fragments
 access-list 110 deny tcp any any
 access-list 110 deny udp any any
 access-list 110 permit ip any any
!
!

```

```

!  

!  

control-plane  

!  

!  

!  

!  

!  

!  

!  

!  

!  

!  

!  

!  

line con 0  

    exec-timeout 0 0  

line aux 0  

    exec-timeout 0 0  

    speed 115200  

line vty 0 4  

    login  

!  

scheduler allocate 20000 1000  

!  

end

```

- CSCsi68795

Symptoms: A PE that is part of a confederation and that has received a VPNv4 prefix from an internal and an external confederation peer, may assign a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

Conditions: The symptoms are observed when receiving the prefix via two paths from confederation peers.

Workaround: There is no workaround.

Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order that the multiple paths for this VPNv4 prefix are learned. The immediate impact is that the local label allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsj10601

Symptoms: Under specific conditions, the new standby supervisor engine may reset repeatedly after a redundancy switchover.

Conditions: The symptom is observed after a redundancy switchover following the below configuration sequence on the active supervisor:

1. frame-relay switching
2. .frame-relay intf-type dce
3. no frame-relay switching

Workaround: Enable **frame-relay switching** on the active and reset the standby.

- CSCsj34557

Symptoms: Router displays following error message and reloads:

```
Jun 18 06:12:23.008: event flooding: code 10 arg0 0 arg1 0 arg2 0

%SYS-3-OVERRUN: Block overrun at E5D8310 (red zone 00000000) -Traceback=
0x6080CEB0 0x60982108 0x60982EC0 0x6098511C 0x609853BC
%SYS-6-MTRACE: mallocfree: addr, pc
662B5B1C,608A6F3C          0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
662B5B1C,608A6F3C          0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
%SYS-6-MTRACE: mallocfree: addr, pc
662B5B1C,608A6F3C          0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
662B5B1C,608A6F3C          0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
%SYS-6-BLKINFO: Corrupted redzone blk E5D8310, words 6088, alloc 61FE2638,
InUse, dealloc 80000000, rfcnt 1 -Traceback= 0x6080CEB0 0x609681D4 0x6098211C
0x60982EC0 0x6098511C 0x609853BC
%SYS-6-MEMDUMP: 0xE5D8310: 0xAB1234CD 0xFFFE0000 0x0 0x63894208
%SYS-6-MEMDUMP: 0xE5D8320: 0x61FE2638 0xE5DB2D0 0xE5D8144 0x800017C8
%SYS-6-MEMDUMP: 0xE5D8330: 0x1 0x0 0x1 0x64B53478

%Software-forced reload
```

Conditions: This symptom occurred on a Cisco 7200 running the c7200-ik9s-mz.124-7a.bin image.

Workaround: There is no workaround.

- CSCsj48472

Symptoms: QoS takes ATM interface default bandwidth for all calculation even when vbr-nrt is set.

Conditions: Occurs on a Cisco 7500 router configured for ATM+QoS.

Workaround: There is no workaround.

- CSCsj49293

Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

Workaround: There is no workaround.

Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsk28361

Symptoms: A 4000 virtual-template (VT) takes high CPU during system load configuration.

Conditions: Occurs when 4000 VT interfaces are loaded from TFTP to running configuration.

Workaround: There is no workaround.

- CSCsk30567

Symptoms: A Cisco 12000 series router with Eng5 line cards may not pass traffic when acting as an Autonomous System Border Router (ASBR) in an Inter-AS VPN Option B configuration.

Conditions: Occurs when VPN routing/forwarding (VRF) is removed from the ASBR. The MPLS labels advertised on the eBGP peering for the VPNv4 prefixes are not programmed in the line cards, so traffic is dropped. The label for a prefix can be seen on the route processor, but not on the line cards. This occurs when there are numerous prefixes in the BGP and with PRP2 with Eng5 line cards.

Workaround: Disable and enable the affected prefix. This updates the labels on the line cards.

- CSCsk64158

Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>.

- CSCsk99687

Symptoms: A router may crash.

Conditions: The symptoms are very rare, but if it occurs it will be seen during ISSU runversion.

Workaround: There is no workaround.

- CSCsl04835

Symptoms: A route introduced by Conditional Route Injection is not removed from the iBGP peer upon withdrawal.

Conditions: Consider this situation: Router B is a BGP router that has two eBGP peers, Router A and Router C. In a situation where RTR_A advertises a prefix and RTR_B injects a more specific prefix of it, the symptom is observed in two ways:

1. If RTR_A withdraws the advertised prefix, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.
2. If the conditional route injection configuration is removed on RTR_B, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.

Workaround: There is no workaround.

- CSCsl13043

Symptoms: Hub in VPN routing/forwarding (VRF) drops ingress multicast when Cisco Express Forwarding (CEF) is enabled on Dynamic Multipoint VPN (DMVPN) tunnel.

Conditions: This happens on a Cisco 7200 router running Cisco IOS Release 12.4(17.9)T.

Workaround: There is no workaround.

- CSCsl13104

Symptoms: Recursive static routes are not being resolved. The **show ipv6 rpf** command does not show the recursion count in the RPF recursion count field.

Condition: This symptom occurs when nonlooping recursive IPv6 static mroutes are configured. This symptom is triggered when IPv6 is configured with PIM Sparse-Mode. The impact of this symptom is that Multicast traffic flow is affected.

Workaround: There is no workaround.

- CSCsl21168

Symptoms: A router crashes. Prior to the crash, the log file contains numerous messages indicating:

```
SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (2/2), process = IP NAT Ager.
```

Conditions: This symptom is observed on a router with NAT enabled.

Workaround: There is no workaround.

Further Problem Description: The fix for this defect caused a new bug: CSCso62511. Ensure that you have the fix for CSCso62511 in addition to this defect if you are encountering this problem.

- CSCsl34481

Symptoms: Router crashes due to IPv6 multicast routing.

Conditions: This happens after applying multicast routing configurations, and again while unconfiguring.

Workaround: There is no workaround.

- CSCsl42627

Symptoms: When sf/ami/56 is configured, the protocol interface is down at both ends.

Conditions: The symptoms are observed when we configure speed 56, framing sf and linecode ami at both ends, as shown:

service-module t1 timeslots all speed 56

service-module t1 framing sf

service-module t1 linecode ami

This causes the protocol to be down and an increased error count at both ends.

Workaround: Change the speed to 64 and then configure again to 56. The protocol will then be up and ping is OK.

- CSCsl44476

Symptoms: Executing a **show flash** command causes high CPU.

Conditions: This symptom is typically seen when there are more than 500 files on the flash.

Workaround: There is no workaround.

- CSCsl49628

Symptoms: When a VPN routing/forwarding (VRF) is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

Conditions: This symptom is observed when BGP is enabled on the router.

Workaround: There is no workaround.

- CSCsl51495

Symptoms: A memory leak may be observed on the standby node.

Conditions: The symptom is observed only when broadcast accounting is configured in the standby node. The memory leak is verified by using the **show processes memory | i AAA ACCT** command.

Workaround: There is no workaround.

- CSCsl58881

Symptoms: A Cisco 2950 switch or any Cisco router may crash unexpectedly.

Conditions: This symptom occurs under the following scenario:

- Cisco Discovery Protocol (CDP) is enabled globally.
- The **show cdp neighbor** command is executed on the CLI.
- The Cisco 2950 is connected to Cisco IP Phones.
- A third party power-over-Ethernet adapter powers the IP Phones.

Workaround: Disable CDP.

- CSCsI92316

Symptoms: Router may experience mwheel CPUHOG condition.

Conditions: This condition is observed on Cisco router while clearing all L2TP sessions when there are more than 2500 sessions with multicast traffic flowing on the sessions.

Workaround: There is no workaround.

- CSCsI96577

Symptoms: The **show ppp multilink** statistics are not updated on a Cisco 7500 router.

Conditions: This symptom is observed when dLFIoLL+SSO is configured on the Cisco 7500 router and a switchover is performed.

Workaround: There is no workaround.

- CSCsI97384

Symptoms: Router reload is seen in the network with a traceback when the **show aaa user all** command is executed.

Conditions: This symptom occurs when the command is executed with 2k or more sessions in progress.

Workaround: Do not enter the **show aaa user all** command.

Further Problem Description: This is more like a timing or race condition, which could occur with a large number of sessions.

The **show** command outputs data from General DataBase which is typically a hash table for each session. However, it does not lock the table during the display for each session. When we have a large number of sessions, the output process may take more than one pass. Meantime if we clear the session, we free the memory associated with that session's General DB. Now, pointers the **show** command is using, point to a freed memory resulting in a reference to a bad pointer. The output process has to sleep (suspend) a moment, and the crash occurs.

- CSCsI99275

Symptoms: High CPU can be seen on Cisco AS5400XM after given uptime.

Conditions: Occurs after 2-3 weeks uptime. CPU usage increases because of "Background Load" process.

Workaround: Reload the access server.

- CSCsm03452

Symptoms: A Cisco AS5850 that is configured as a SIP gateway may crash unexpectedly when running a high volume of SIP calls.

Conditions: This symptom is observed on the Cisco AS5850.

Workaround: There is no workaround.

- CSCsm17767

Symptoms: On a gateway configured for ISDN Non-Facility Associated Signaling (NFAS) with a primary and backup D channel, both the primary and backup D channel interfaces may be marked “OUT OF SERVICE” if the gateway sends the first “in-service” message during a D channel switchover.

Conditions: This symptom occurs only when the gateway sends the first ISDN service message indicating that it is bringing the backup D channel in service. If the peer sends the message first, the switchover is completed successfully.

Workaround: There is no workaround.

- CSCsm21335

Symptoms: When the **cm-manager config server <ip address>** is used, router fails to configure or misconfigures the gateway voice ports. This results in non-functional voice ports.

Conditions: Occurred on a Cisco 3845 running the c3845-advipservicesk9-mz.124-13d.bin image. Example of the errors follow:

```
voice-port 1/0/0
  signal unknown <--- should have been default loop start
  ring frequency unknown <--- should have been default ring freq
  timing hookflash-in 400 20
  shutdown <--- should have been no shut
```

In addition, PRI E1 trunks fail with no dial tone yet there is no indication why. The Cisco OS configuration looks OK.

Workaround: Do not use these commands. Configure the MGCP gateway manually.

- CSCsm26610

Symptoms: A router running Cisco IOS may unexpectedly reload.

Conditions: This is specific to platforms with powerpc processors, such as the npe-g2 and 2600xm series routers. It requires either the legacy rate-limit config or MQC style policer configured on an interface.

Workaround: There is no workaround.

- CSCsm50741

Symptoms: When a non-DC router is removed from a DC enabled area and the area becomes DC enabled, some of the LSAs are not refreshed correctly with DoNotAge (DNA) bits set. Crash may happen when customer deploys iptivia probes in the network. Fixed in CRS.

Conditions: The symptom is observed when a router without DC capability is removed from a DC enabled area.

Workaround: Use the **clear ip ospf** command.

- CSCsm55817

Symptoms: When configuring ATM PVCs, under the PVC syntax you can provide a handle to describe the PVC. If this handle starts with “00” (zero zero) then the command will fail.

Conditions: The symptom is observed when configuring ATM PVCs and where the PVC handle starts with “00”.

Workaround: Do not use handles that start with “00”.

- CSCsm80048
Symptoms: Policy on MFR interface stays in suspend mode after a **shut/no shut** even though required bandwidth is available.
Conditions: Occurs with a QoS policy attached to MFR interface on a Cisco 7500 router.
Workaround: There is no workaround.
- CSCsm89795
Symptoms: The router keeps reloading and complaining about unavailability of memory.
Conditions: This symptom is observed if the router is directly connected to a DHCP server or if an attack is made by flooding DHCP replies.
Workaround: There is no workaround.
- CSCsm96785
Symptoms: You may observe a problem which the OSPF neighbor is down after switch-over in spite of using OSPF Non-Stop Forwarding (NSF).
Conditions: This occurs with the following conditions:
 - “nsf cisco” is only affected. If “nsf ietf”, this problem does not occur.
 - You may observe this problem if the OSPF interface is “point-to-multipoint non-broadcast” or “point-to-multipoint”. If the interface is “broadcast”, this problem does not occur.
 - When this problem occurs after switch-over, DBD packet may not be exchanged between two neighbors. And the neighbor is down in spite of NSF.
 Workaround: Change the OSPF config to “nsf ietf” and change the OSPF interface to “broadcast”.
- CSCsm96842
Symptoms: The command **hold-queue length in** cannot be configured for port-channel interface.
Conditions: The symptom is observed with a Cisco 7600 series router after upgrading to Cisco IOS Release 12.2(33)SRC.
Workaround: There is no workaround.
Further Problem Description: Queueing is not supported for port-channel with a Cisco 7600 series router. The hold-queue is a legacy queueing command and is not supported.
- CSCso01307
Symptoms: On a Hot Standby Router Protocol (HSRP) standby router, all accounting records for **aaa accounting commands** and **aaa accounting system** on the standby router of the HSRP pair are available only if those two commands are applied.
Conditions: AAA accounting is configured on a router pair that is running HSRP.
Workaround: Change the router to the active state before making changes that are to be logged.
Further Problem Description: The following message will appear when the **debug aaa accounting** command is executed and a record is suppressed:


```
*<time/date>: AAA/ACCT/CMD(00000003): Suppressed record
```
- CSCso19662
Symptoms: Tracebacks are seen after unconfiguration when using the **clear ip nat translation *** command.
Conditions: This traceback occurs with the c7200-js-mz.124-18a.fc2 image.
Workaround: There is no workaround.

- CSCso28309

Symptoms: Ping fails from reflector during internal testing.

Conditions: The goal of the test is to verify the successful termination of PPP/PPPoE over ATM sessions on router's ATM interface using auto sensing. It is performed with auth_pap, process switch, and keepalive disabled. This has a functional impact as the virtual access entry is not getting added to the routing table after doing clear ip route.

Workaround: There is no workaround.

- CSCso51519

Symptoms: Paths with same next-hop may be marked as being multipath.

Conditions: The symptom is observed when multipath is configured and when using RRs in the environment.

Workaround: There is no workaround.

- CSCso54167

Symptoms: BGP peers are stuck with table versions of 0. BGP peers do not announce any routes to neighbors.

Conditions: Whenever the interfaces flap with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

Workaround: Delete and reconfigure the neighbor.

- CSCso62166

Symptoms: Device crashes while debugging Border Gateway Protocol (BGP) IPv6 unicast updates entering the **clear bgp ipv6 uni *** command.

Conditions: Debugging must be on to see the crash

Workaround: Use the **no debug bgp ipv6 unicast update** command to turn off BGP IPv6 unicast updates debugging.

- CSCso64050

Symptoms: Policy-map outputs are not seen in standby router. The policy is attached to the VC in the standby, but no output is seen.

Conditions: The symptom is observed when an ATM PVC is created and a service policy is attached to the PVC.

Workaround: There is no workaround.

- CSCso69584

Symptoms: On a CMM running Cisco IOS Release 12.4.13b with an ACT Module, several DSPs may get reset because of heartbeat errors and may cause the calls to fail. The following messages will be displayed on the console, and traceback messages may also appear:

```
Apr 3 11:59:09: ac_mtrDsp_ev(slot 0 dspId 1 heartBeat 0CDC8D38) reset[hbErr 0]
Apr 10 10:54:41: ac_mtrDsp_ev(slot 1 dspId 2 heartBeat 10718287) reset[hbErr 0]
Apr 10 10:54:41: ac_mtrDsp_ev(slot 2 dspId 1 heartBeat 107178F7) reset[hbErr 0]
Apr 10 10:54:56: ac_mtrDsp_ev(slot 2 dspId 1 heartBeat 0000058D) reset[hbErr 0]
Apr 10 10:54:56: ac_mtrDsp_ev(slot 1 dspId 2 heartBeat 000005BF) reset[hbErr 0]
Apr 10 10:55:12: %SCHED-2-EDISMSCRIT: Critical/high priority process MS_AC Dsprm Main
may not dismiss.
-Process= "MS_AC Dsprm Main", ipl= 0, pid= 38
```

Conditions: This symptom is observed under normal working conditions and occurs because of unknown reasons.

Workaround: There is no workaround.

- CSCso73533

Symptoms: Traceback is seen after unconfiguring the tunnel interface.

Conditions: The symptom is seen when using Ipv4 multicast PIM tunnels where the route to the Rendez-Vous Point (RP) is via another tunnel interface. If this tunnel interface was unconfigured, then there is a race condition between:

1. learning about the new route to the RP via another interface
2. periodic update of the PIM tunnel adjacency. If the latter occurs first the traceback is seen

Workaround: There is no workaround.

- CSCso74028

Symptoms: The local PE is sending graft messages even after receiving data from the remote PE on an MVPN network.

Conditions: This symptom is observed when the graft-ack messages are lost in transit (could be due to misconfiguration/ACL, etc.).

Workaround: Fix the misconfiguration so that graft-ack messages are forwarded as expected.

- CSCso78897

Symptoms: A Cisco 870 router will process and forward packets received with a multicast MAC address even though it should not, such as when the interface controller does not own the multicast MAC address.

Conditions: This was observed on a Cisco 878 Router running Cisco IOS Release 12.4(15)T4.

Workaround: Make sure the switch connecting to the Cisco 870 does not send packets with multicast MAC addresses that should not be received by the Cisco 870.

- CSCso89794

Symptoms: Spurious accesses are seen when SNMP queries are performed on the router.

Conditions: This symptom occurs if SNMP queries like “snmpwalk -v2c 7.42.19.43 public .1.3.6.1.4.1.9.3.6.13.1” are performed on the router. Spurious accesses are seen.

Workaround: There is no workaround.

- CSCsq02587

Symptoms: Traffic engineering (TE) tunnel is not coming up in MPLS TE.

Condition: Occurs when both Ethernet Over MPLS (EoMPLS) and MPLS TE are configured on the router.

Workaround: There is no workaround.

- CSCsq03286

Symptoms: A Cisco Communication Media Module (CMM) with an Adhoc Conferencing and Transcoding (ACT) port adaptor module configured for MTP/XCODING may get into a state where further attempts to utilize DSP resources in a transcoding profile may fail.

Conditions: Under rare conditions, a CMM module used for MTP/XCODING may see the DSP resource on the module become unresponsive. When this occurs, a DSP recovery algorithm on the CMM module will be invoked to attempt to recover the DSP resource.

This algorithm may in some circumstances leave the associated transcoding resource in a state where further calls to invoke these resources will fail.

When the DSP recovery mechanism is invoked, the following message at debug level will be logged:

```
ac_mtrDsp_ev(slot 2 dspId 1 heartBeat 0000058D) reset[hbErr 0]
```

If the recovery mechanism fails to properly recover the resources, there will be hung calls seen in the output of the **show mediacard connection** command (0 packets tx/rx will be displayed).

Further calls that attempt to use this resource will see OpenReceiveChannel failures as displayed in the output of the **show sccp statistics** command.

An example of this is below:

```
CMM-01# show mediacard connection
```

Id	Type	Slot/ DSP/Ch	RPort	SPort	RxPkts	TxPkts	Remote-IP
25	xcode	2/4/23	18300	22684	0	0	172.16.175.160
26	xcode	2/4/24	16710	22540	0	0	172.16.175.116

```
CMM-01# show sccp statistics
```

```
SCCP Application Service(s) Statistics:
```

```
Profile Identifier: 1, Service Type: Transcoding
TCP packets rx 1676, tx 443
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 1, successful 1, rejected 0, failed 0
KeepAlive tx 25, successful 25, failed 0
OpenReceiveChannel rx 412, successful 398, failed 24
CloseReceiveChannel rx 412, successful 398, failed 14
StartMediaTransmission rx 412, successful 398, failed 14
StopMediaTransmission rx 412, successful 380, failed 0
Reset rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

Workaround: Work to prevent the DSP from becoming unresponsive.

- CSCsq05099

Symptoms: User can only configure a maximum of 500 SWMTP sessions per profile.

Conditions: This symptom is observed when using SWMTP.

Workaround: Configure multiple SWMTP profiles.

- CSCsq06813

Symptoms: Only one RELEASE message is seen on a DHCPv6 when the server is shut, even though multiple messages are expected.

Conditions: The symptom occurs on Cisco 7200 series router that is running Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCsq09942

Symptoms: NM-CEM-4TE1 modules installed in Cisco 3845 routers running 12.4.11T or 12.4.15T3 codes with nine TS CEM groups configured have alignment issues. When the issue occurs, all **show cem** commands do not show any problems with the cards or CEM groups.

Conditions: This symptom is observed on an NM-CEM-4TE1 module installed in Cisco 3845 routers with nine TS groups configured and connected to another vendor PBX.

Workaround:

1. Shut/no shut the CEM group on either side. This fixes the issue temporarily.
2. Change the CEM group configuration to have one TS per CEM group.

Further Problem Description: The issue can be observed with more details using a WAN analyzer between the CEM card and the PBX. There you can see that the traffic is entering through a specific TS and leaving through a different TS.

- CSCsq12128

Symptoms: If the WAN connection is DOWN on the VGW, the Media Gateway Control Protocol (MGCP) fallback mode may not load. The gateway remains in “MGCP Fallback mode: Enabled/OFF” mode.

Conditions: This symptom is observed with Cisco IOS Release 12.4(16).

Workaround: Shut down the interface.

Further Problem Description: It is possible that the link goes up and down frequently. The call manager application tries to download the XML file from CCM+TFTP even when the link is down. This sets a flag. The flag prevents the fallback.

- CSCsq13938

Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. This bug affects BGP **show** commands related to VPNv4 address family. In each case the problem only happens if the deconfiguration removes objects that are being utilized by the **show** command. Removing unrelated BGP configuration has no effect.

This bug is specific to MPLS-VPN scenarios (CSCsj22187 fixes this issue for other address-families).

Workaround: Terminate any paused BGP **show** commands before beginning operations to remove BGP-related configuration. Pressing “q” to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

- CSCsq14031

Symptoms: Unable to ping IP address of session target. Packets of certain sizes (between 57 and ~63 bytes, depending on the type of packet) are corrupted when using a tunnel over a PPP multilink interface. EIGRP packets were within this range and so were dropped and caused the route to the IP address being pinged not to be added.

Conditions: Issue may be related to encryption or Network Address Translation (NAT).

Workaround: Disable or increase the value of **ppp multilink fragmentation**.

- CSCsq14294

Symptoms: Standby router keeps reloading in RPR+ mode.

Conditions: The symptom is observed when distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) is configured on MC-STM1 and MTU size is changed on multilink members.

Workaround: Change MTU back to 1500.

- CSCsq22106

Symptoms: All CAS voice calls fail on a Cisco AS5850 box. This failure is not seen on PRI calls.

Conditions: This symptom is observed for CAS calls but not for PRI calls.

Workaround: There is no workaround.

- CSCsq24935

Symptoms: A switch reloads when the **distance bgp** command is configured under ipv6 address family.

Conditions: This symptom is observed on a Cisco 3560 that is running Cisco IOS Release 12.2(44)SE2. The same symptom is also seen on a Cisco 3750. The following commands are issued:

```
router bgp <>
  address-family ipv6 unicast
  distance bgp <> <>
```

The router subsequently reloads because of an Instruction access Exception.

Workaround: There is no workaround. BGP/ipv6 is not supported on such platforms.

- CSCsq29139

Symptoms: When IPv6 prefix delegation receives periodic RENEW message from a client, it may incorrectly bind the corresponding prefix for another client.

Conditions: The symptom is observed when IPv6 prefix delegation assigns a prefix to a client that is connected via a virtual access interface.

Workaround: There is no workaround.

- CSCsq29623

Symptoms: A Cisco AS5350 or Cisco AS5350XM that is running Cisco IOS Release 12.4(15)T5 will drop incoming VPN traffic larger than 512 bytes when the traffic is destined for a dialer interface.

Conditions: Conditions where problem is seen:

- When packets arrive on a crypto tunnel that terminates on the Cisco AS5350 AND when the packets are destined for a destination that is reachable over a dialer interface.
- With a legacy dialer-map or dialer-pool DDR configuration. No difference is seen between the two.
- With CEF disabled.

Conditions where problem is not seen:

- Without crypto.
- With process-switching (CEF and fast-switching disabled).
- When packets are destined for a host that is reachable via an Ethernet interface.

Workaround: There is no workaround.

- CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsq33653

Symptoms: The caller ID transmission may fail from FXS port to FXO port.

Conditions: The symptoms are observed when the sub-command **caller-id** is configured under “voice-port x/y”.

Workaround: There is no workaround.

- CSCsq34171

Symptoms: A router may crash when the IP address/mask is changed on the interface.

Conditions: The symptom occurs if EIGRP authentication is enabled.

Workaround: Disable authentication.

Further Problem Description: When the authentication is removed from the interface, the crash does not occur on changing the mask.

- CSCsq44052

Symptoms: When configuring “is-type level-1” under “router isis”, the following error message may be received:

```
% Ambiguous command: "is-type level-1"
```

Conditions: The symptom is observed when configuring “is-type level-1” under “router isis”.

Workaround: There is no workaround.

- CSCsq44598

Symptoms: A PA-POS-2OC3 experiences an output stuck condition.

Conditions: This issue is sporadic in nature and is sometimes seen with QoS configurations although QoS is not the cause of the issue. The issue is due to an extra interrupt, which is confusing the driver if it expires before the FIFO reaches the low point. For example, if the FIFO goes full but is filled with large packets, then it is possible that the no traffic timer will expire before the tx packets have emptied. It is a communication issue between the hardware and the driver code.

Workaround: There is no workaround.

- CSCsq46336

Symptoms: Radio transmissions from LMR voice ports to PMCs may intermittently drop packets in the router.

Conditions: The symptom is seen where multiple PMC users monitoring the same stream cause more than three simultaneous RTP streams to be present on the LMR router.

Workaround: If customer is running PMC, turn off the keepalive on the PMCs.

- CSCsq47980

Symptoms: Router crashes while attempting OCSP revocation check.

Conditions: The symptom is seen on a Cisco router that is running Cisco IOS Release 12.4(21).

Workaround: There is no workaround.

- CSCsq52483

Symptoms: A memory leak may occur when using the **dot1x port-control force-authorized** command.

Conditions: The symptom is observed on a Cisco 831 router that is running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCsq52630

Symptoms: Router may not boot up and the following error message may be shown: program section linked to illegal address

Conditions: The symptoms are observed on a Cisco 820 series router and a Cisco 828 router that is running Cisco IOS Release 12.4(21).

Workaround: There is no workaround.

- CSCsq53910

Symptoms: A Cisco router may reload due to a bus error crash:

```
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x411E79C0
-Traceback= 0x411E79C0 0x411E8260 0x411D2C74 0x411D34F0 0x411D4B34 0x411D4CD8
0x423520C8 0x408BE970 0x408C25BC 0x408B7878 0x41215404 0x41231530 0x426D86F0
0x426CAFC8 0x42348C98 0x42348C7C
```

Conditions: The symptom is seen on a Cisco 2821 router that is running Cisco IOS Release 12.4(18). The crash appears to be triggered when the command **no ccm-manager** is entered.

Workaround: There is no workaround.

- CSCsq55070

Symptoms: Traceback occurs while testing AAA Authentication and Asynchronous Call (ACQ) feature.

Conditions: Occurs on a Cisco 3745 running Cisco IOS Release 12.4 and Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCsq60016

Symptoms: A router crashes after a long RSA key string is entered.

Conditions: This symptom is observed when a very long hex string is entered.

Workaround: Break the entry into shorter strings.

- CSCsq62703

Symptoms: Intermediate System-to-Intermediate System (IS-IS) tries to access invalid memory address and may cause router to stop working.

Conditions: Occurs when a switch over happens and standby router becomes active.

Workaround: There is no workaround.

- CSCsq63731

Symptoms: If either the command **vlan-id dot1q vlan-id** or the command **vlan-range dot1q start-vlan-id end-vlan-id** is configured on a main interface which is also configured for routing, and an ARP packet is sent to the router on the configured VLAN, then the router may send an ARP reply with a VLAN ID of zero.

Conditions: The symptoms are seen on a Cisco 2800 series and a Cisco 7200 series router when the command **vlan-dot1q vlan-id** is configured on the GigabitEthernet interface of a Cisco 2800 series router and **encapsulation dot1q vlan-id** is configured on the FastEthernet 2/1/2.1 interface.

Workaround: Change the Cisco 2800 series router's (CE) configuration to use a sub-interface for the VLAN-ID instead of using the **vlan- dot1q** *vlan-id* command on the main interface. With a sub-interface configured on the 2800, we can verify that the ARP packets are sent with proper VLAN ID.

- CSCsq70473

Symptoms: An MWAM processor Gigabit Ethernet interface stops processing traffic.

Conditions: This symptom is observed at a high rate of incoming traffic.

Workaround: Restart the interface (enter the **shutdown** command followed by the **no shutdown** command) to restore traffic forwarding.

- CSCsq71095

Symptoms: SSL connection over L2TP IPSec tunnel does not work. Checksum errors on the Change Cipher Spec messages coming from the server.

Conditions: This has been seen on a Cisco 7200 running Cisco IOS Release 12.4(15)T5 and the ADVENTERPRISEK9-M image. A Cisco 2821 with the same version and feature set was not affected.

Workaround: Use a router other than the Cisco 7200 for this task, or disable IPSec and only use SSL over L2TP.

- 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.

- CSCsq73514

Symptoms: The transform-set assigned to a crypto map may be truncated.

Conditions: The symptom is observed with a transform-set when configured manually via CLI and when assigned a name greater than three characters.

Workaround: Limit transform-set name to three characters or less.

- CSCsq74300

Symptoms: Loopbacks, Null0, and other non-Point-to-Point interfaces are not allowed in a **route-map set** command because of the changes introduced with caveat CSCsk63775.

Conditions: This symptom is observed with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsq75787

Symptoms: Cannot enable AutoQoS on ATM subinterface.

Conditions: This happens on a Cisco 3800 router that is running Cisco IOS Release 12.4(15)T6.

Workaround: There is no workaround.

- CSCsq76349

Symptoms: On an incoming call from PSTN, the beginning of a conversation may intermittently be missed.

Conditions: The symptom is observed on a Cisco AS5800 that is controlled via MGCP, and is running Cisco IOS Release 12.4(13)e.

Workaround: There is no workaround.

- CSCsq83872

Symptoms: There may be a memory leak when the **no pppoe enable** command is applied.

Conditions: This symptom is observed on a Cisco 831 router.

Workaround: There is no workaround.

- CSCsq94036

Symptoms: Packets are hardware-switched after applying IP precedence. The expected behavior here is that packets are software-processed when “ip precedence” is applied over “ip next-hop” because applying a policy over the other wipes the adjacencies that were already established.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SX or Release 12.2SR.

Workaround: There is no workaround.

- CSCsq98586

Symptoms: Router emits traceback after the **source-bridge ping 4095 15 4095 vmac xxxx.xxxx.xxxx** command is entered.

Conditions: Happens after configuring the command **source-bridge ring-group xxxx** and try **source-bridge ping 4095 15 4095 vmac xxxx.xxxx.xxxx**.

Workaround: There is no workaround.

- CSCsq98742

Symptoms: Cisco AS5400 router crashes frequently with Cisco IOS Release 12.4 (19b) attempting to free memory for X28 component.

Conditions: This symptom is observed on a Cisco AS5400.

Workaround: There is no workaround.

- CSCsr06282

Symptoms: Causes router to reload following a SNMP get operation.

Conditions: Only occurs when a DHCP operation is configured with option-82 parameters.

Workaround: Do not query MIB objects relating to the DHCP operation configured with option-82

- CSCsr08476

Symptoms: Trying to remove the MFR bundle crashes the router.

Conditions: After OIR, remove the VIP (those VIP interfaces are members of MFR bundle). Try to remove the MFR bundle.

Workaround: There is no workaround.

Further Problem Description: The MFR bundle has one Channelized PA interface as a member. OIR remove that PA seated VIP and next try to remove the bundle using the **no int MFR** command. The router crashes.

- CSCsr10221

Symptoms: Hub router may crash after establishing 250 or more IPSec tunnels.

Conditions: The symptom is observed with 250 or more DMVPN tunnels with traffic flowing in them. It is seen when a QoS service policy is associated with the spokes which are up.

Workaround: There is no workaround.

- CSCsr11514

Symptoms: QoS RTP statistics are not updated correctly for a short call duration.

Conditions: Call flow:

PSTN ---(E1)---> AS5850 -(MGCP)----> Call Agent.

- Calls are less than 40 seconds.
- The **show voice active** command has not been issued (will force update).
- The RTCP timer is set to 65000.

Workaround: Reduce the **ip rtcp report interval** value on the gateway, and monitor the load.

- CSCsr13521

Symptoms: Memory chunk allocated for LDP-IGP Sync may leak.

Conditions: The symptom is observed on a router with a dual link to its neighbor. LDP and LDP Graceful Restart are enabled on both routers. When LDP is disabled and re-enabled globally on the neighbor router, a small memory leak occurs on this router.

To verify the memory leak, on Router 1, enable memory leak debug with the **set memory debug incremental starting-time** command. On Router 2, disable LDP globally with the **no mpls ip**. Wait for LDP session go down, then re-enable LDP. On Router 1, the memory chunk leak for LDP should be seen with the **sh mem debug leaks chunks** command.

Workaround: There is no workaround.

- CSCsr17315

Symptoms: Autoinstall process does not run correctly with a BOOTP or DHCP server in same LAN. Because of the problem, the configuration file may not be downloaded using TFTP from the network during autoinstall.

Conditions: The symptoms are observed with a Cisco 7200 series router that is running Cisco IOS Release 12.4(21.06)T01. It is observed with a BOOTP server and when the DHCP client and TFTP server are in same LAN. The client is configured to obtain an IP address for an interface (using the **ip address dhcp** command) and then the DHCP client configuration is copied to TFTP. The autoinstall process is started using “write erase and reload”. It shows that no BOOTP information is received. The DHCP client downloads the hostname.config file from TFTP. As a result, the configuration (using the **ip address dhcp** command) is missing on the interface.

Workaround: There is no workaround.

- CSCsr19440

Symptoms: A router crashes if the **zone cluster local** command is configured with a cluster ID that is an empty string.

Conditions: This symptom is observed when the local cluster ID and the local zone associated with the cluster are an empty string and when the **no service alignment detection** command is configured.

Workaround: Configure the local cluster ID and the local zone associated with the cluster with a nonempty string. Also, configure the **service alignment detection** command to prevent the crash.

- CSCsr20566

Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

Workaround: There is no workaround.

- CSCsr20889

Symptoms: The system reloads.

Conditions: The symptom is observed when a dynamic crypto map is added to the existing GETVPN crypto map with a different sequence.

Workaround: There is no workaround.

- CSCsr23454

Symptoms: A device reloads with a bus error and may display the following message:

```
CMD: ' aggregate-address 224.0.0.0 224.0.0.0 attribute-map GCI-aggregations
suppress-map Suppress-ESNAK' 16:19:05 GMT Wed Jun 18 2008
```

```
16:19:06 GMT Wed Jun 18 2008: Address Error (load or instruction fetch)
exception, CPU signal 10, PC = 0x60CDD444
```

Conditions: The symptoms are observed on a device configured with Border Gateway Protocol (BGP).

Workaround: There is no workaround.

- CSCsr27734

Symptoms: The standby router crashes.

Conditions: This symptom is observed when a service-policy map is removed from a VC.

Workaround: There is no workaround.

- CSCsr38532

Symptoms: A memory leak is observed in the CCH323_CT process when a load test is performed.

Conditions: This symptom is observed with Cisco IOS Release 12.4(18b) but not with Cisco IOS Release 12.4(19b).

Workaround: There is no workaround.

- CSCsr48828

Symptoms: A Cisco router may display the following traceback: %SYS-2-GETBUF

Conditions: The symptom occurs when ACLs are configured on the WAN interfaces of the router. When outbound packets fail and are dropped on an outbound ACL, a traceback is generated. If the packets are stopped or the ACLs removed, the tracebacks stop. The problem is seen with the VSA accelerator, but not seen when software crypto is used.

Workaround: There is no workaround.

- CSCsr49376

Symptoms: Device Reloads after EIGRP adjacency changes.

Conditions: Occurs on a Cisco Catalyst 3560 running Cisco IOS Release 12.2(44)SE. This has been observed on several other devices also. At this stage, the root cause has not been found.

Workaround: There is no workaround.

- CSCsr54272

Symptoms: Spurious memory and traceback is observed on a Cisco 5850 upon a gateway crash.

Conditions: The problem is seen when a gateway is handling voice and fax calls.

Workaround: There is no workaround.

- CSCsr55278

Symptoms: Fast switching of multicast packets may not occur on the interface of a PE router. All multicast packets are forwarded in process switching.

Conditions: The symptom is observed after the interface is changed from a forwarding interface of one VRF to another VRF.

Workaround: There is no workaround.

- CSCsr55713

Symptoms: A crash occurs.

Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

Workaround: There is no workaround.

- CSCsr59242

Symptoms: EIGRP may lose some routes from stub neighbors in a DMVPN setup.

Conditions: If EIGRP graceful restart happens on an interface and the interface update queue is busy, then it may lose some routes from the stub neighbors on that interface.

For example, issuing the below commands can trigger this issue:

clear ip eigrp vrf abc as-number neighbors interface Wait 30 seconds **clear ip eigrp vrf abc as-number neighbors interface soft**

Workaround: Use the **clear ip eigrp vrf abc neighbors** command to fix the problem.

Another workaround is that graceful restart can be turned off by the **no eigrp graceful-restart** command under the router or the **address-family** command. This will cause the symptom to go away but will revert back to hard resetting peers on configuration changes or the **clear ip eigrp neighbor soft** command.

- CSCsr61729

Symptoms: WIC-2AM-V2 and WIC-1AM-V2 card is recognized but the ping functionality may be broken.

Conditions: The symptoms are observed with a back-to-back connection of WIC-2AM-V2 and WIC-1AM-V2 modules with a third-party vendor connector.

Workaround: There is no workaround.

Further Problem Description: The problem is due to a prior checkin which made the state of the device dependent on the physical connection of the cable. This code was interfering with the software state machine which internally maintains the state of the machine.

- CSCsr62441

Symptoms: Router is crashing while configuring “connect *word* voice-port 7/0:0 t1 7/0” and tracebacks can be observed.

Conditions: The symptoms are observed on a Cisco 5400 platform when configuring “connect *word* voice-port 7/0:0 t1 7/0”.

Workaround: There is no workaround.

- CSCsr62797

Symptoms: A router may crash when traffic is triggered between peers.

Conditions: The symptom is observed when two IPSec flows under each IKE SA are configured. If one IPSec flow is kept idle for each IKE SA and traffic is triggered between the peers, the router will crash.

Workaround: Do not configure the idle-timer for crypto ipsec security- association.

- CSCsr65344

Symptoms: The following traceback may be seen after loading Cisco IOS Release 12.4(21):

```
%SYS-2-INTSCHED: 'sleep for' at level 2 -Process= "Init"
```

Conditions: The symptom is observed on a Cisco RSP8 (R7000) processor or a Cisco RSP16 (R7000A) processor that is running Cisco IOS Release 12.4(21).

Workaround: There is no workaround.

- CSCsr67177

Symptoms: A router may experience a corner case crash if an IPv6 OSPF router is removed from the configuration.

Conditions: The following conditions must be met before router is removed from the configuration to experience the system crash:

- OSPFv3 router does not run because the router-id is not available (it means that no IP address is available and/or router-id is not configured).
- SW interface is configured, assigned under inactive OSPFv3 router, and later removed using the **no interface** command.

Workaround: Ensure that when the IPv6 router is configured it runs properly (if it does not start, there is a warning printed on the console advising what action to take).

- CSCsr83547

Symptoms: Dialer watch on the Cisco 3845 router makes the backup link of PPP multilink on the PRI port which is connected to BRI 4 port of peer router through ISDN net. If one out of four BRI ports is shut down on the peer router, the dialer watch does not keep the backup link up without resetting the idle timer at the expiration of idle timeout though the primary link remains down, causing the other three ports to be disconnected.

Conditions: This symptom occurs only when the BRI port which contains B-ch that became link up first is shut down. This symptom does not occur even if the other BRI ports are shut down.

Workaround: There is no workaround.

- CSCsr87229

Symptoms: Callers that use a caller-ID length of 15 characters or greater cannot call out of analog MGCP ports.

Example:

```
MGCP Packet received from --->
CRCX 132 AALN/S0/SU1/0@nicmatth-ipipgw MGCP 0.1
C: A000000001000026000000F5
X: 23
L: p:20, a:PCMU, s:off, t:b8
M: recvnly
R: L/hd
```

```
S: L/rg, L/ci(08/08/15/44,1002,This is my long name)
Q: process,loop
<---
```

MGCP Packet sent to --->

510 132 unsupported caller id length

Conditions: The BELLCORE standards support only 15 characters, and the MGCP gateway disconnects the call because of unsupported caller-ID length and displays the following message:

510 unsupported caller id length.

Workaround: Configure a caller ID less than 15 character, or use the port with SCCP or H323 to prevent this. Also, the following cptones are not affected: “FR”, “DE”, “NO”, “IT”, “ES”, “ZA”, “TR”, “GB”, “AT”.

- CSCsr96753

Symptoms: A router may crash when entering the **isdn test call** command.

Conditions: The symptom is observed when the BRI interface is up.

Workaround: There is no workaround.

- CSCsr97030

Symptoms: Service policy is missing from the running-configuration after a device is reloaded.

Conditions: The symptom is observed when the service policy contains a “police rate percent” that is 13% or less, and is applied to an MLPPP interface. It is observed with Cisco IOS Release 12.4(8c) and Release 12.4T.

Workaround: Use any one of the following:

1. Re-apply service-policy each time after rebooting.
2. Change service policy to use “police rate XXXX bps”.
3. Configure bandwidth XXXX on the MLPPP interface.
4. Change service policy to use more than 13% for the policing.

- CSCsu02176

Symptoms: A router reloads continuously on switching off one of the redundant power supplies.

Conditions: This symptom occurs when a router reloads continuously on switching off one of the redundant power supplies.

Workaround: There is no workaround.

- CSCsu03608

Symptoms: A Cisco 7500 series router may crash.

Conditions: The symptom is observed when we try to bring up the ATM-IMA interface.

Workaround: There is no workaround.

- CSCsu04446

Symptoms: A Cisco router that is running a PfR Master Controller crashes under stress.

Conditions: This symptom is observed when traffic with more than 2000 prefixes with about 500 unreachable prefixes is flowing through the router.

Workaround: Minimize the number of prefixes learned during an interval. The default of 100 should be sufficient.

oer master learn prefixes 100

- CSCsu06350

Symptoms: T.38 fax call not terminating audio properly.

Conditions: RE-INVITE from SIP Fax application changes connection IP address in SDP. PGW sends changed IP address in MDCX to GW. GW responds with 200 acknowledging this change. GW still sends audio to IP address where original call terminated.

Workaround: There is no workaround.

- CSCsu10042

Symptoms: A Cisco 7206VXR router may crash periodically. An error message similar to the following (using the **show version** command) may be seen: System returned to ROM by bus error at PC 0x605663D8, address 0xFFFFFFFF4

Conditions: The symptoms are observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(16). It is observed when MPLS-aware Netflow is configured along with **ip flow-capture mac-addresses**.

Workaround: De-configure **ip flow-capture mac-addresses**.

Further Problem Description: This issue is also seen with Cisco IOS Release 12.4(21).

- CSCsu27888

Symptoms: IGMP v3 reports are discarded.

Conditions: Occurs on Cisco 7200 router running Cisco IOS Release 12.4(20)T2.

Workaround: There is no workaround.

- CSCsu31954

Symptoms: A router reloads.

Conditions: Under certain crypto configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsu36836

Symptoms: TCL scripts and policies attempting to work with open files and sockets simultaneously may not operate properly. One symptom is the **vwait** command may fail by reporting “would wait forever”.

Conditions: Occurs when a TCL script opens both a file and a client or server socket simultaneously.

Workaround: Open and close files and sockets separately. Avoid having them open simultaneously.

- CSCsu38520

Symptoms: In Cisco IOS Release 12.4(20)T and 12.4(15)T7, IKE Phase 1 is not flushed by DPD (although IKE Phase 2 is correctly deleted). This can be verified by using the following commands: **show crypto isakmp sa** then **show crypto ipsec sa**

Conditions: The symptom is observed when the IPSec end node is behind NAT and DPD is configured. It is seen when the last IKE Phase 2 SA is deleted.

Workaround: Use Cisco IOS Releases up to 12.4(15)T6.

- CSCsu51095

Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

Conditions: This symptom can occur if, for some reason, PfR is learning connected routes or if the user has configured them.

Workaround: Create an oer-map with a prefix-list that contains the prefixes with the IP addresses of the connected routes (the next hops). Set the set observe mode in the oer-map.

- CSCsv40404

Symptoms: When DDNS is disabled on the router, which is configured as the DHCP server, it sends option 81 in the DHCP ACK message with the N flag bit set to 1. But the DHCP Client fails to understand this and does not do PTR update. The issue is seen with a DNS server and a Cisco IOS DHCP server.

Condition: The issue is not seen with the Cisco IOS Release 12.3 code as it does not support DDNS and does not reply back with Option 81 in the DHCP ACK.

Work around: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(21a)

Cisco IOS Release 12.4(21a) is a rebuild release for Cisco IOS Release 12.4(21). The caveats in this section are resolved in Cisco IOS Release 12.4(21a) but may be open in previous Cisco IOS releases.

- CSCsm03452

Symptoms: A Cisco AS5850 that is configured as a SIP gateway may crash unexpectedly when running a high volume of SIP calls.

Conditions: This symptom is observed on the Cisco AS5850.

Workaround: There is no workaround.

- CSCso19662

Symptoms: Tracebacks are seen after unconfiguration when using the **clear ip nat translation *** command.

Conditions: This traceback occurs with the c7200-js-mz.124-18a.fc2 image.

Workaround: There is no workaround.

- CSCsq12128

Symptoms: If the WAN connection is DOWN on the VGW, the Media Gateway Control Protocol (MGCP) fallback mode may not load. The gateway remains in “MGCP Fallback mode: Enabled/OFF” mode.

Conditions: This symptom is observed with Cisco IOS Release 12.4(16).

Workaround: Shut down the interface.

Further Problem Description: It is possible that the link goes up and down frequently. The call manager application tries to download the XML file from CCM+TFTP even when the link is down. This sets a flag. The flag prevents the fallback.

- CSCsq83872

Symptoms: There may be a memory leak when the **no pppoe enable** command is applied.

Conditions: This symptom is observed on a Cisco 831 router.

Workaround: There is no workaround.

- CSCsr20566

Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(21)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(21). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(21). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCee21263

Symptoms: Non-initial fragments may be dropped by the reflexive ACL.

Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCeg05149

Symptoms: After a secondary image is loaded by Standby, “NVRAM Verification Failed” messages show up on Standby console resulting in lost startup and private configuration.

Conditions: The problem is seen only on a Cisco RSP platform that is running Cisco IOS 12.2SB versions.

Workaround: Issue the **write memory** command as soon as slave comes up.

- CSCek37305

Symptoms: A router crashes when unconfiguring a T1 controller with an interface configured for RTP priority.

Conditions: This symptom has been seen on a Cisco 7200 NPE-G1 router loaded with Cisco IOS interim Release 12.2(31.4.17)SB.

Workaround: Ensure that the **ip rtp priority** or **ip rtp reserve** command is removed before deleting the interface.

- CSCek57749

Symptoms: Execution of the **show version** or **show hardware** commands during traffic may result in packet drops.

Conditions: This symptom occurs when executing the **show version** or **show hardware** commands.

Workaround: There is no workaround.

Further Problem description: Disabling NETIO interrupts/executing interrupt handlings of higher priority than NETIO interrupts have always been a source of packet drops on Cisco 7200 (as is the case with other uni-processor systems, for example CSCed10454). The drops usually occur due to lack of descriptors.

The **show version** and its constituent functions make use functions which are implemented as exceptions, which are user generated exceptions of higher priority than any interrupts.

- CSCek65374

Symptoms: The PRE3 may not parse the startup configuration.

Conditions: This symptom is observed on a Cisco router that has dual RPs.

Workaround: There is no workaround.

- CSCek74855

Symptoms: Modifying class parameters in a service policy attached to a multilink may trigger a crash, if the **show policy-map int** command is issued.

Conditions: The problem is platform independent, but it has been seen on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(13.13)T.

Workaround: There is no workaround.

- CSCek75931

Symptoms: A Cisco 10000 series router may experience a CPUHOG condition.

Conditions: This condition is observed when there is an increase of more than 2000 sessions established.

Workaround: There is no workaround.

- CSCek78237

Symptoms: A short CPU hog seen in the ATM PA Helper process when an interface flaps and the framing configuration is modified on the interface.

Conditions: This symptom is observed on a Cisco 7200 with a PA-A3-T3 adapter that is running Cisco IOS Release 12.2(25)S or 12.2(31)SB (and possibly other Cisco IOS releases).

Workaround: There is no workaround.

Further Problem Description: The CPU hog is enough to cause OSPF adjacencies (with fast hello) to go down on other unrelated interfaces. The same problem is seen if BFD is configured.

- CSCsb98277

Symptoms: A Cisco 7500 router may pause indefinitely after an interface reset.

Conditions: This symptom is observed on a Cisco 7500 router that is configured with input QoS service policy together with Distributed Link Fragmentation and Interleaving over Leased Line. It occurs when the **shutdown** and **no shutdown** commands are used.

Workaround: There is no workaround.

Further Problem Description: This bug fix implements enhancement in scheduling QoS classes with bandwidth less than 1% of the link rate, same as CSCdz40273.

- CSCse03637

Symptoms: PIM dense mode interoperability issues are seen with Cisco and third party boxes.

Condition: This symptom is observed when PIM dense mode is in operation. After the multicast forwarder is decided, based on the assert mechanism, a prune is erroneously sent. Multicast stream ceases to flow.

Workaround: There is no workaround.

- CSCse61834

Symptoms: When you modify an ATM PVC by entering the **pvc vpi/vci** command, any subsequent modifications in the VC class that is assigned to this PVC do not take effect.

Conditions: This symptom is observed when the PVC is preconfigured with a VC class when the following events occur:

- 1) You make a configuration change in the PVC.

2) You change the configuration in the VC class.

The configuration change in the VC class does not take effect.

Workaround: First complete the configuration changes in the VC class. Then, change the configuration in the PVC.

- CSCse90710

Symptoms: A Versatile Interface Processor (VIP) may crash while configuring T1 or E1.

Conditions: This symptom is observed with a VIP in which a PA-MC-8T1E1 port adapter is installed that is configured with either a T1 or an E1 controller.

Workaround: There is no workaround.

- CSCsf32449

Symptoms: A Sup720 Multicast-VPN (MVPN) PE router may not advertise its mdt prefix (BGP vpnv4 RD-type 2) after reloading.

Conditions: This symptom is observed on a Sup720 MVPN PE router.

Workaround: Use the **clear ip bgp** command after reloading.

- CSCsg98535

Symptoms: The **clear ipv6 pim topology** command may crash the router.

Conditions: The symptom is observed when using the **clear ipv6 pim topology** command on the router with 30,000 (S, G) multicast (mroute) state.

Workaround: Do not use **clear ipv6 pim topology** when the router has 30,000 mroute state. Rather, wait for three or more minutes for the mroute state to timeout and the router will remove the entry from the mroute table.

- CSCsh79893

Symptoms: A Cisco 2800 router running zone-based firewall and URL filtering may reload.

Conditions: Occurs when URL filtering is unconfigured or reconfigured under the policy map during periods of high traffic.

Workaround: There is no workaround.

- CSCsi03359

Symptoms: A PIM hello message may not reach the neighbor.

Conditions: This symptom is observed on a Cisco router when an interface comes up and a PIM hello message is triggered.

Workaround: Decrease the hello timer for PIM hello messages.

Further Problem Description: The symptom occurs because the PIM hello message is sent before the port can actually forward IP packets. IGP manages to get its neighborship up but PIM does not, causing RPF to change to the new neighbor and causing blackholing to occur for up to 30 seconds.

- CSCsi04335

Symptoms: While using HTTP based authproxy authentication for large number of sessions, it is possible for some sessions to get stuck in unauthenticated state.

Conditions: The problem is seen when large number of users(200+) try to login to the network with a burst rate of 5 sessions/second.

Workaround: There is no complete workaround for this problem. But the customers can try the following. a) Identify the sessions that are in INIT state using **show ip auth- proxy cache** command. b) Clear the sessions using **clear ip auth-proxy** command.) Identify the TCP sessions associated

with the above users by using the **show tcp brief** command, and clearing the TCB by using the **clear tcp tcb Address** identified using the **show tcp brief** command. By using the above workaround the customers can ask the users to try to login again, and if the load on the box is not significant then it is possible for the user to complete the authentication.

- CSCsi83521

Symptoms: A Cisco 7200 router crashes upon execution of a sequence of permit commands under “ipv6 access-list testipv6” subconfiguration mode.

Conditions: This symptom is observed on a Cisco 7200 router that is loaded with a Cisco IOS Release 12.4(13.13)T3 image.

Workaround: There is no workaround.

- CSCsi86823

Symptoms: An incorrect NAS port ID is found while testing IDBless VLAN for PPPoE.

Conditions: The symptom is observed on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsi93916

Symptoms: An alignment error (i.e., spurious memory access) that causes tracebacks such as “ipnat_nbss_is_special_packet” may be observed on a Cisco router.

Conditions: The symptoms are observed with a certain packet format, not yet identified. It is specific to the NetBios Session Service (NBSS) protocol.

Workaround: There is no workaround.

- CSCsj21785

Symptoms: A Traffic Engineering (TE) tunnel does not re-optimize to explicit path after an MTU change.

Conditions: The TE tunnel is operating via explicit path. The MTU on outgoing interface is changed. OSPF is flapped, and it does not come up as there is MTU mismatch (MTU is not changed on peer router). Meanwhile the TE re- optimizes to a dynamic path-option as expected. Now the MTU is reverted back to the previous value, and the OSPF adjacency comes up. The TE tunnel does not re-optimize to explicit path. Manual re-optimization of the TE tunnel fails as well, and the TE tunnel sticks to the dynamic path.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the particular interface.

- CSCsj54606

Symptoms: Invalid updates to the system clock are allowed on the Cisco IOS command line interface (CLI).

Conditions: The symptoms are observed when a user attempts to configure the set end of summer-time earlier than the start of summer-time:

```
Router(config)#clock summer-time PDT date 11 mar 2007 2:00 ?
<1-31>  Date to end
MONTH   Month to end
```

```
Router(config)#$r-time PDT date 11 mar 2007 2:00 11 march 2007 00:00 60
```

Workaround: Do not pass invalid arguments to the **clock summer- time** command on the Cisco IOS CLI.

- CSCsj78403

Symptoms: A router may crash when the **clear ip bgp** command is entered.

Conditions: Occurs on devices running BGP and configured as a route reflector client with conditional route injection configured.

Workaround: Unconfigure conditional route injection.

- CSCsj93012

Symptoms: A router may crash when QoS is enabled.

Conditions: This symptom is seen with IMA ATM interfaces on Cisco 7500 and Cisco 7200. Occurs when ATM and serial interfaces have QoS configurations as output/input policy and when peer is reloaded/or write memory is done. This is specific to IMA .

Workaround: There is no workaround.

- CSCsj93374

Symptoms: A secondary processor may crash when one is copying a file onto a subdirectory in a slavedisk from the master and at the same time renames the subdirectory and then deletes the file from the slave console.

Conditions: This symptom is observed on a Cisco router that has an ATA file system.

Workaround: Do not rename the subdirectory and delete the file when it is being copied to the subdirectory.

- CSCsk21764

Symptoms: A Cisco router may reload unexpectedly due to a bus error crash.

Conditions: The symptoms can be observed when the router is running Voice XML.

Workaround: There is no workaround.

- CSCsk26651

Symptoms: A router crashes when configuring auto QoS on an ATM subinterface. The following error message is produced:

```
"%SYS-6-STACKLOW: Stack for process Exec running low"
```

Conditions: The symptom occurs when AutoQoS Discovery is enabled for untrust mode, and also when AutoQoS Discovery is enabled for trusted DSCP.

Workaround: There is no workaround.

- CSCsk28748

Symptom: When an IMA group subinterface (atm1/ima1.14016) is configured before a **no shut** is done on the IMA group interface, the maximum value VBR-NRT peak cell rate (PCR) option is displayed as 1536/1920(T1/E1) instead of 1523/1904.

Conditions: Occurs when IMA group subinterface is configured before assigning ATM interface to the IMA group.

Workaround: Configure the IMA group interface first and then configure image group sub- interface.

- CSCsk36324

Symptoms: On a Cisco router, OSPF might go into a loop during SPF calculation, causing high CPU utilization and rendering the router inaccessible.

Conditions: This symptom occurs when router LSAs with a link metric disallowed by RFC 2328 are present in the network (note that Cisco routers do not originate such LSAs) and when the network is unstable (link flapping during the SPF calculation).

Workaround: To fix the problem, reload the router. To prevent the problem, manually configure a link metric according to RFC 2328.

Important Note: CSCsk36324 caused MPLS TE defect CSCsl18176 and has been backed out under defect CSCsl18176. A new fix for this issue will be committed under defect CSCsl32318.

- CSCsk40676

Symptoms: The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Conditions: Occurs when LZS compression is used on a Windows Vista client.

Workaround: Disable LZS compression.

- CSCsk54061

Symptoms: Memory allocation failed atm_vpivci_to_vc error occurs and device crashes.

Conditions: Occurs while configuring for ATM-AutoVC or with incoming ATM traffic.

Workaround: There is no workaround.

- CSCsk54092

Symptoms: Link-state advertisement (LSA Type 3) may not get flushed from the database when the route is suppose to be included as LSA Type 5.

Conditions: This symptom is observed when an LSA is changed from type 3 to type 5 on a Cisco router. This is a timing problem between OSPF and BGP. Routes redistributed into OSPF are shown as Type 3 LSAs when the **sh ip ospf process-id database** command is entered, even after the removal of the **network** command under the router which is advertising these routes. These routes are to be learned via Type 5 LSAs. This problem exists in all branches except Cisco IOS Release 12.2S.

Workaround: Configuring the PE routers in different domains using the **domain-id A.B.C.D** command can solve the issue.

- CSCsk61790

Symptoms: Syslog displays password when copying the configuration via FTP.

Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

Workaround: There is no workaround.

- CSCsk63655

Symptoms: A Media Gateway Control Protocol (MGCP) gateway may return a 524 or 510 error code with the reason as “invalid local connection option” for a valid “L:” parameter in a CRCX message.

Conditions: The symptoms can be observed on a router that is running Cisco IOS Interim Release 12.4(17.4)T1 or later, when the **debug mgcp parser** command with verbose tracelevel is disabled.

Workaround: Enable **debug mgcp parser** with verbose tracelevel.

- 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.

- CSCsk75147

Symptoms: A cbs3120 switch may crash during license installation, while reloading the slave switch that is being installed with license.

Conditions: The symptoms are observed when: 1. Installing up to 10 licenses in one file on Slave 4 in one vty session. 2. Reloading Slave 4 while installing the license on another vty session.

Workaround: There is no workaround.

Further Problem Description: The issue is related to Inter-Process Communication (IPC). The crash is due to accessing an already freed port info. But the crash may be prevented by adding a check `atcipc_notify_session_closure`.

- CSCsk86150

Symptoms: When EIGRP goes down, BGP installs the major network in the routing table. When EIGRP comes up again, it installs the subnet routes in the routing table, while the BGP major network remains in the routing table. Also, the BGP local source route is not installed in BGP table.

Conditions: Occurs on routers running Cisco IOS Release 12.4(10b) and 12.4(13c) Enterprise Services images.

Workaround: Reconfigure the network command

- CSCsk98507

Symptoms: Router crashes after IPX routing is enabled.

Conditions: Problem happens only if an interface which has IPX network configuration is deleted after disabling IPX routing.

Workaround: There is no workaround.

- CSCsl04516

Symptoms: A Cisco router may experience the following errors:

```
%TCP-2-INVALIDTCB: Invalid TCB pointer: 0x476292F0 -Process=
"Skinny Socket Server", ipl= 0, pid= 260 -Traceback= 0x41259724 0x41A50418
0x41A54754 0x41A28134 0x41A2AFA4 0x41A2F30C 0x4095AB80 0x4095B5F4 0x423CD6E4
0x423CD6C8
```

```
%TCP-2-INVALIDTCB: Invalid TCB pointer: 0x476292F0 -Process=
"Skinny Socket Server", ipl= 0, pid= 260 -Traceback= 0x41259724 0x41A50418
0x41A54754 0x41A28134 0x41A2AF24 0x41A2F30C 0x4095ABA4 0x4095B5F4 0x423CD6E4
0x423CD6C8
```

Phones that are running over secure channels will have registration problems.

Conditions: This symptom occurs on a Cisco 2821 router that is running Cisco IOS Release 12.4(18).

Workaround: There is no workaround.

- CSCsl08480

Symptom:

The following error messages are seen Memory allocation failed atm_vpivci_to_vc with subsequent device crash.

Conditions: Observed with incoming ATM traffic.

Workaround: None.

- CSCsI09904

Symptoms: The Bootstrap Router message (BSM), with RP information and holdtime of zero, creates a group-mapping state when the RP information does not exist.

Conditions: The symptoms are observed in internal negative testing in an IPv6 multicast environment. Trigger is when a packet with an RP holdtime of zero is sent.

Workaround: There is no workaround.

- CSCsI10459

Symptoms: Routers that are running Cisco IOS Release 12.4(13b) and Release 12.4(16) may crash when the **show crypto pki timers** command is executed.

Conditions: This symptom is observed under a narrow set of conditions. Offending conditions occur when certificates are issued Certificate Distribution Point formatted in URL format. Certain other unknown circumstances must also occur.

Workaround: Avoid using the **show crypto pki timers** command.

- CSCsI14450

Symptoms: Under a high load of multicast traffic, a Cisco router may unexpectedly reload due to a CPU vector 300 or bus error.

Conditions: This symptom has been observed only in environments where more than 10 tunnels have been configured on the same device using multicast over these tunnels.

Workaround: There is no workaround.

- CSCsI17539

Symptoms: A Cisco router may reload with the following symptoms:

```
%SYS-3-MGDTIMER: NZ prev pointer but not running, timer = 64C37818. -
Process= "IP Input", ipl= 4, pid= 66 -Traceback= 0x60746048 0x6084EA34 0x6084F14C
0x62333AD8
0x62337C70 0x62306494 0x623068B0 0x60A40654 0x60A416F8 0x60A41778 0x60A41964 Oct 31
22:55:48.894: %SYS-3-MGDTIMER: Setting zero expiration time, timer = 64132350.
-Process= "IPSEC
key engine", ipl= 4, pid= 150 -Traceback= 0x60746048 0x6084E9A8 0x6084FA18

22:55:48 zulu Wed Oct 31 2007: Address Error (load or instruction fetch) exception,
CPU signal 10, PC =
0x60815B08

0x60815B08 0x6084FCA4 0x622B2E54 0x622B39C4
```

Conditions: Occurred on a Cisco 7206VXR running Cisco IOS Release 12.4(16).

Workaround: There is no workaround.

- CSCsI22080

Symptoms: WebVPN hangs after a few days of working. When this happens, no WebVPN connections are active and no new connections can be established. The **debug ip tcp transaction** command shows **connection queue limit reached: port 443** errors. The **show tcp brief** command displays many sessions in SYNRCVD and TIMEWAIT states. Problem is recovered either by reload or by entering the **clear tcp tcb *** command. There are few stale sessions in CLOSED state left after clearing TCP.

Conditions: Issue seen in Cisco IOS Release 12.4.15T and Cisco IOS Release 12.4.15T1 when WebVPN is configured. The issue is intermittent and happens after few days or weeks of working.

Workaround: To restore TCP connectivity, issue **clear tcp tcb *** or reload the router. Note that this will clear all TCP sessions on the router.

- CSCsl25732

Symptom: GPRS tunneling protocol (GTPv1) periodic interim accounting records are not sent out by device.

Conditions: Occurs when using GTPv1 PDP together with AAA periodic interim accounting configuration.

Workaround: None.

- CSCsl27236

Symptoms: WS-C6506-E with WS-SVC-IPSEC-1 keeps crashing with error %SYS-3-CPUHOG: Task is running for (126000)msec This is a CPU HOG SW forced crash.

Conditions: The symptoms can be observed under stress conditions and when ipsec-isakmp is enabled.

Workaround: There is no workaround.

Further information: This is a day one bug that just surfaced. The customer found this under heavy stress conditions. The node list is getting corrupted, hence will iterate through the list indefinitely causing the CPU hog.

- CSCsl27704

Symptoms: Interfaces remain down after using the **clear service module** command on an interface with the **loopback remote** command initiated. Also the **show service- module** command may show ambiguous output.

Conditions: The symptoms can be observed when the **loopback line** or **loopback dte** commands are initiated and cancelled before initiating the **loopback remote full** command.

Workaround: Reload the router.

Further Problem Description: Procedure HWIC-1DSU-T1-----HWIC-1DSU-T1

1. Connected HWIC-1DSU-T1 back to back as shown in setup
2. Initiate loopback line on (s0/3/0) 3825 for HWIC-1DSU-T1
3. Cancel loopback line - cancelled successfully
4. Initiate loopback remote full on (s0/3/0) 3825 for HWIC-1DSU-T1
5. Clear service module s0/3/0 on 3825 6. It does not cancel loopback remote successfully and both interface s0/3/0 of 3825 and 3845 are down. Both end shows unexpected information in **show service- module** “remote loopback (remotely initiated) is in unknown” state.

- CSCsl32142

Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with “Bad getbuffer” error may also be reported.

Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCsl40687

Symptoms: Router reloads due to a bus error. This occurs with the following messages:

```
%ALIGN-1-FATAL: Illegal access to a low address 08:32:13 AEST Tue Nov 20 2007
addr=0xB8, pc=0x40099888 , ra=0x44020000 , sp=0x465870E8
```

```
08:32:13 AEST Tue Nov 20 2007: TLB (store) exception, CPU signal 10, PC =
0x40099888
```

```
-Traceback= 0x40099888 0x402F6358 0x415102F4 0x41510C7C 0x402FF5C4 0x414F1140
0x402FF7B8 0x41C8B8E0 0x41C8EFC0 0x41C8F064
```

```
0x41C85260 0x421EA0C4 0x421EA224
```

Conditions: This occurs after applying a Modular Quality of Service Command-Line Interface (MQC) class on a PVC.

Workaround: Use frame relay traffic shaping (FRTS) instead of MQC under the PVC.

Further Problem Description: MQC policy is not a supported configuration for MLPoFR connections. The above configuration is not valid. Currently, the MQC policies are configurable under MLPoFR PVCs and this results in router reload. However, the router should not crash even under those circumstances. This fix prevents MQC QOS policy from being configured on MLPoFR connections at config time when MLP may not yet be active. So, in effect, the config is blocked both if MLP is active or if MLP is just configured.

- CSCsl50271

Symptoms: An Open Shortest Path First (OSPF) enhancement, to avoid a suspend when link state update packets are sent, may result in a router crash.

Conditions: The symptoms are observed in a scenario with 3k tunnels. Both unconfiguring the loopback interface and deleting the loopback interface trigger the same code path that may lead to OSPF suspension.

Workaround: There is no workaround

Further Problem Description: The problem actually exists in all branches. However, this is a timing issue.

- CSCsl58230

Symptoms: 100% CPU utilization at the interrupt level is observed on a Cisco router following an upgrade from Cisco IOS Release 12.3(8)YG5 to Release 12.3 (8)YG6.

Conditions: The symptom is observed on a Cisco 837 router.

Workaround: The only workaround is to not upgrade to Cisco IOS Release 12.3 (8) YG6 from Release 12.3(8)YG5.

- CSCsl61416

Symptoms: Certain prompts will not play properly. Dead air is heard and call disconnects.

Conditions: Occurs on a Cisco AS5350 acting as a VXML gateway in an IPCC environment and running Cisco IOS Release 12.4(7)b using streaming prompts.

Workaround: Turn off streaming mode. Reloading the gateway temporarily fixes the issue.

- CSCsl62609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsl63494

Symptoms: AAA server does not count active user sessions correctly. User authentication may be denied by the AAA server because max session limit has been reached.

Conditions: This may occur with AAA authentication, when max session limit is configured on Cisco Secure ACS server (may happen with other AAA servers too). When user initiates X.25,ssh,rsh,rlogin or telnet sessions and later disconnects them, AAA server does not decrement active sessions counter due to wrong attributes present in the accounting records sent by the device. Eventually, the misbehaving counter may reach max session limit, and user will be denied a login.

Workaround: Removing max session limit can be considered.

- CSCsl70143

Symptoms: Under heavy traffic, ISDN calls may be rejected due to high CPU usage with the following messages seen in the log (with tracebacks):

```
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (98/100).
Call (callID=23524) is rejected.
```

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (32/18),process
= ISDN.
```

Conditions: This problem occurs only under heavy traffic.

Workaround: There is no workaround.

- CSCsl71540

Symptoms: Router reloads when the **sh ip bgp options** command is entered.

Conditions: This is seen in releases where CSCsj22187 is fixed.

Workaround: There is no workaround.

- CSCsl77158

Symptoms: A Cisco router may see the following errors:

```
Oct 30 16:42:04.094 GMT: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x405039FC
reading 0x1678
```

Conditions: The symptoms may be observed on a CISCO7513 running Cisco IOS Release 12.0(32)S3 with PA-MC-E3 cards installed.

Workaround: There is no workaround. This problem is not service impacting.

- CSCsl78850

Symptoms: When the WAN is restored between an MGCP/SRST gateway and CallManager, the MGCP gateway intermittently fails to register back with CallManager.

Conditions: Connectivity to the CallManager from the gateway is stopped. When the gateway goes in SRST, a PSTN call is placed to a phone that registers with the gateway. WAN connectivity is then restored. MGCP has one primary call agent and two redundant hosts configured.

Workaround: Reload the gateway.

Further Problem Description: When the gateway is in this “stuck” state of not registering with the CallManager, if “no ccm-manager mgcp” is configured, it does not take effect, and “no ccm-manager redundant-host ...” also does not take effect. The following error message is displayed:

```
cmapp_service_emptying_redun_hostlist: Error: cannot execute CCM host change -- must
configure again!
```

- CSCsI80870

Symptoms: While bringing up 20 MLPoATM bundles with 10 member links, a few member links fail to come up.

Conditions: This symptom occurs when some of the member links are inactive when the bundles come up.

Workaround: There is no workaround.

Further Problem Description: The cause for this issue is the bundle auth type does not match with the current links auth type. The current link name does not match the bundle first link name. CONFREJ is sent, and the member is removed from the bundle.

- CSCsI80887

Symptoms: The router may crash and there is high CPU usage if the Routing Information Protocol's (RIP) minimum update interval is configured to zero.

Conditions: The symptom may be observed on a Cisco router using RIP version 2 process, with the timer values set to 0 1 0 1.

Workaround: Do not configure RIP's minimum update interval to zero.

- CSCsI81170

Symptoms: When adding a static NAT translation, a permanent ARP entry is added. When configuring multiple translations for the same address and removing one, the ARP entry is removed even though there may be a NAT translation that still requires it.

Conditions: The symptoms are observed when there are multiple translations with the same addresses, for example:

```
ip nat inside source static tcp 192.168.2.1 20 192.168.4.5 20 extendable
ip nat inside source static tcp 192.168.2.1 21 192.168.4.5 21 extendable
```

Workaround: Remove and re-add the NAT configuration lines for the IP address.

- CSCsI82444

Symptoms: The T.38 fax relay may fail to send all pages of a fax.

Conditions: The symptom can be observed when we send Real-Time Transport Protocol (RTP) and Non-RTP packets simultaneously. T.38 fax protocol uses User Datagram Protocol (UDP) for fax and the initial session establishment is by RTP.

Workaround: Using Cisco fax relay will solve the problem.

- CSCsI83415

Symptoms: After executing the following CLI commands (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

```
Test10 :
-----
a. clear ip bgp 10.0.101.46 ipv4 multicast out
b. clear ip bgp 10.0.101.47 ipv4 multicast out
```

Test 1:

```
c. show ip bgp ipv4 multicast nei 10.0.101.2
d. show ip bgp ipv4 multicast [<prefix>]
e. config terminal
```

The crash does not happen for each of the following cases:

1. If the same CLI is cut-paste manually, there is no crash.
2. If the **clear cli** command is not executed, there is no crash.
3. If the **config terminal** command is not entered, there is no crash.

Conditions: The symptom occurs after executing the above CLI.

Workaround: There is no workaround.

- CSCs187400

Symptoms: H323 setup message is malformed after NAT translation

Conditions: Setup message includes the neededFeatures, desiredFeatures, supportedFeatures extensions.

Workaround: Do not use the extensions listed above.

- CSCs190187

Symptoms: Low memory leak may occur on VoIP gateway in VTSP process, which may cause router to reload.

Conditions: The issue is specific to the C549 DSPs on Cisco 3700 series routers. The leak occurs when a call is disconnected due to non-availability of the circuit (cause code 0x22).

Workaround: There is no workaround.

- CSCs192595

Symptoms: After 3 minutes of normal operation, packet loss occurs over Dialer PPP multilink (MLPPP enabled) interfaces.

Conditions: Occurs when CEF is enabled and “ip address negotiated” is configured on the interface.

Workaround: Use one of the following options: Permanent: disable CEF with the **no ip cef** command. Permanent: configure a static IP address on the interface. Temporary: Use the **clear adj** command to refresh all adjacencies (will last 3 minutes).

- CSCs195431

Symptoms: A router may reload when malformed packets are sent to the TFTP UDP port.

Conditions: This symptom is observed when malformed traffic is sent to the router’s TFTP UDP port 69 (TFTP). The TFTP server port must be listening within Cisco IOS software.

TFTP port 69 is opened in Cisco IOS software under the following circumstances:

- TFTP-Server is explicitly enabled with the command: **tftp-server filename**.

For further information on TFTP server functionality, see:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_file-transfer_ps63_50_TSD_Products_Configuration_Guide_Chapter.html#wp1000933

- E-phones are configured if Cisco Unified Communications Express (CME) is being used and e-phones are configured port UDP 69 (TFTP) will be opened within Cisco IOS software. If the configuration contains **ephone-dn arguments**, then port 69 is opened.

For further information on the CME e-phone functionality, see:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmebasic.html#wp1013086

Workaround: There is no workaround. However, the following mitigation may be suitable for some customer environments:

Infrastructure ACLs (iACL)

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 to 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, which will protect all devices with IP addresses in the infrastructure IP address range:

```
!--- Permit TFTP (UDP port 69) packets
!--- from trusted hosts destined to infrastructure addresses.

access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq tftp

!--- Deny TFTP (UDP port 69) packets
!--- from all other sources destined to infrastructure addresses.

access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq tftp

!--- 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 here:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

- CSCsI96254

Symptoms: If an EIGRP distribute-list applied to an interface allows a route, the route will be installed into the routing table without first checking to see if the global distribute-list allows it as well. All platforms are affected.

```
access-list 1 permit any
access-list 2 deny any
```

```

router eigrp 1
 network 192.168.1.0 0.0.0.255
 distribute-list 1 in FastEthernet0/0
 distribute-list 2 in
 no auto-summary

```

The above configuration should deny all routes by virtue of access-list 2. Instead, all routes are allowed per ACL 1.

Conditions: Running EIGRP with interface distribute lists and a global distribute list. All platforms are affected.

Workaround: Currently the only workaround is to apply the global distribute list to each interface distribute list as well.

- CSCsl98867

Symptoms: The command **no ip nat service list acl7 ftp tcp port 1009** may not unconfigure the command **ip nat service list acl7 ftp tcp port 1009**.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS software.

Workaround: There is no workaround.

- CSCsl99883

Symptoms: The X.25 PVC experiences window closed on both the sides.

Conditions: The problem is seen under heavy traffic conditions. The testing scenario passes 1000 packets containing 2000 bytes of data.

Workaround: Reset the connection.

- CSCsm01126

Symptoms: The standby fails to come up in SSO. The following message is seen on the active:

%FILESYS-4-RCSF: Active running config access failure (0) <file size>

Conditions: This symptom is observed when the router has a configuration greater than 0.5 megabytes.

Workaround: There is no workaround.

- CSCsm04442

Symptoms: Delete an interface which has ip summary-address rip configured. The router crashes.

Conditions: In the scenario where different summary addresses are configured for different interfaces, if we delete an interface that has a summary-address configuration which is the last one for that summary-address that it leads to.

Workaround: Remove the **ip summary-address rip** configuration from an interface which is going to be deleted.

- CSCsm08010

Symptoms: A Cisco IOS VG224 voice gateway may reload unexpectedly if an FXS voice port configured with the **caller-id enable** command, receives a call where the calling number (ANI) is greater than 32 digits.

Conditions: The symptom is observed when caller-id is enabled and the ANI is greater than 32 characters in length.

Workaround: The workaround is to disable caller-id in the FXS voice port and restrict the ANI to less than 32 digits.

- CSCsm08030

Symptoms: A router may crash while parsing “x28 profile <profile name>”. This occurs when x28 mode is configured. The crashinfo file will show: %SYS-2-FREEFREE: Attempted to free unassigned memory at [...]

Conditions: This symptom is observed on a Cisco AS5400 gateway that is running Cisco IOS Release 12.4(1c) and Release 12.4(18).

Workaround: There is no workaround.

- CSCsm08291

Symptoms: Virtual access interfaces flap, and the following error message is displayed:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done.
```

Conditions: Occurs on a Cisco 7206VXR with NPE-G2 and running Cisco IOS Release 12.4.(11)T1.

Workaround: There is no workaround.

- CSCsm08398

Symptoms: Negative number is displayed in the output for the **show ip nat translation** command and in rate limiting. This limit entry option fails due to the huge number of entries shown in **ip nat statistics**.

Conditions: In some situations show ip nat statistic calculation falls negative, which shows as huge number by the NAT. Limit entry looks into this number for stop NAT translation. When this is negative limit entry stops NAT from doing translations.

Workaround: There is no workaround.

- CSCsm12247

Symptoms: A Cisco IOS router configured for WCCP may stop redirecting traffic following a change in topology.

Conditions: The router must be configured for WCCP redirection using the hash assignment method. When there is only a single appliance in the service group, the loss of hash assignment details is permanent. However with multiple appliances in the group, the loss of assignment information is transitory; the router soon recovers.

Workaround: To recover the assignment details, the WCCP configuration needs to be removed and re-added to the router. Use the **no ip wccp service** command followed by **ip wccp service args** command.

Additional Information: The changes address also situation where some wccp clients are sending modified weight field in the wccp message and this way create a topology change situation.

Additional Information: The changes address also situation where some wccp clients are sending modified weight field in the wccp message and this way create a topology change situation.

- CSCsm17110

Symptoms: When setting the “FlipAddr” attribute in an IPS signature, one expects the attacker and victim TCP/IP addresses to be swapped. This is not occurring as expected and signature actions will be created against the improper TCP/IP address.

Conditions: Edit an IPS signature and set the “FlipAddr” attribute to True. Receive traffic that should cause the edited signature to fire. If a deny action is configured, the destination/victim TCP/IP address will be used instead of the expected source/attacker TCP/IP address.

Workaround: There is no workaround.

- CSCsm17414

Symptoms: When prompts are being played, the barge-in type-ahead feature works intermittently. During the menu playout, user will make a selection that should stop the rest of the menu from being played. The user is not able to stop the menu playout despite making a selection. Once the menu finishes the prompt accepts the correct digit.

Conditions: Occurred in the Cisco Customer Voice Portal (CVP) VXML application running on Cisco IOS Release 12.4(15)T1. CVP version was 3.1 SR2. CVP VXML Server and Studio 3.1. ICM 7.0 SR4 ES42.

Workaround: Combine two prompts into one.

- CSCsm17711

Symptoms: The **rmdir** command deletes a directory which has files and subdirectories in it. This behavior is not valid.

Conditions: The symptom can be observed when using the **rmdir** command with a USBFLASH filesystem.

Workaround: There is no workaround.

- CSCsm17879

Symptoms: After putting the onboard GE0/0-1 interfaces into promiscuous mode, they still will not accept packets with destination MAC other than the broadcast and the interface MAC.

Conditions: This affects the onboard GE interfaces only.

Workaround: Use FE/GE ports from a module to achieve this, if available.

- CSCsm20351

Symptoms: AAL2 trunk alarm is not generated for a resource availability indication (RAI) condition when a T1 is disconnected from a VWIC module.

Conditions: This issue is seen when AAL2 trunking is configured on a Cisco 2811 running Cisco IOS Release 12.4(17a)

Workaround: There is no workaround.

Further Problem Description: This issue is not seen on non-ISR platforms running Cisco IOS Release 12.3.

- CSCsm20994

Symptoms: Kron occurrences are not rescheduled properly when the clock is set near the end of a calendar year.

Conditions: A kron occurrence is scheduled daily or hourly. The clock is reset near the end of the year such that the next occurrence of the kron policy would happen in the next year.

Workaround: After clock reset, remove/restore kron occurrences to cause them to be scheduled properly.

- CSCsm21335

Symptoms: When the **cm-manager config server ip address** is used, router fails to configure or misconfigures the gateway voice ports. This results in non-functional voice ports.

Conditions: Occurred on a Cisco 3845 running the c3845-advipservicesk9-mz.124-13d.bin image. Example of the errors follow:

```
voice-port 1/0/0
  signal unknown <--- should have been default loop start
  ring frequency unknown <--- should have been default ring freq
```

```

timing hookflash-in 400 20
shutdown <--- should have been no shut

```

In addition, PRI E1 trunks fail with no dial tone yet there is no indication why. The IOS configuration looks OK.

Workaround: Do not use these commands. Configure the MGCP gateway manually.

- CSCsm26130

Symptoms: When removing a subinterface from the configuration that contains an IP address that falls into the major net of the static route, the static route is no longer injected into the BGP table. Since the route is not in the BGP table, it is not advertised to any peers.

Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.

Workaround: There are four possible workarounds:

1. Use an “aggregate-address” configuration instead of the static route to generate the summary.
2. Remove auto-summary from the BGP process.
3. Enter the **clear ip bgp *** command.
4. Remove and reconfigure the BGP network statement for the summary route.

- CSCsm26610

Symptoms: Router with QoS policer applied on the physical interface crashed after traffic starts. The crash causes subsequent crashes even after router is reloaded and when traffic rate is very low.

Conditions: Occurs when 1000 IPsec tunnels are built on the same physical interface configured with the policer. This is specific to Cisco 7200 routers with NPE-G2 processors. This issue is not seen with Cisco 7200s with NPE-G1s or NPE-400s.

Workaround: There is no workaround.

- CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>

- CSCsm27726

Symptoms: After overwriting DHCP pool and client pool, status of client is IDLE.

Conditions: Occurs on Cisco routers running a pre-release version of Cisco IOS Release 12.4(17b).

Workaround: There is no workaround.

- CSCsm27943

Symptoms: When **dls w timer explorer-wait-time** is set, Ethernet redundancy could not establish DLSW circuit sometimes with the following message in the debug:

Jan 15 15:32:22.643 JST: DLSW-ER:(CSM):startdl_pend timer expired for transparent circuit

Conditions: The symptom only occurs when the router is configured for **dls w timer explorer-wait-time** with DLSw Ethernet Redundancy and **dls w transparent switch- support**.

Workaround: There is no workaround.

- CSCsm27958

Symptoms: After upgrading a Cisco 7600 to Cisco IOS Release 12.2(33)SRC, SSO does not come up and router stays in RPR.

Conditions: Occurs only if the **passive-interface default** command is configured under OSPF.

Workaround: After upgrade, unconfigure and configure again the **passive-interface default**.

- CSCsm27979

Symptoms: A router crashes with “Address Error (load or instruction fetch) exception” when the **show ip vrf vrf-name** command is used.

Conditions: On one vty session, enter the **show ip route vrf vrf-name** command and leave it in the “more” condition. From other user interface session, go to configuration mode, and then enter the **no ip vrf vrf-name** command using the same VRF name. After at least 5 minutes, the router will crash after hitting the any key on the session that is doing the **show ip vrf** command.

Workaround: Make sure that there is no **show ip route vrf** command pending before entering the **no ip vrf** command.

- CSCsm34361

Symptoms: TCP ports may not show open as required during port scanning using NMAP.

Conditions: This symptom is observed on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsm34632

Symptoms: PPTP connection does not get established properly. Users are stuck in authentication phase

Conditions: Occurs when PPTP server is behind a NAT router configured with a static NAT entry.

Workaround: There is no workaround.

- CSCsm36524

Symptoms: The aggregation caches are not capturing the correct mask and prefix information. The problem is seen for source prefix only.

Conditions: The symptoms can be observed on a Cisco router that is running Cisco IOS Release 12.4(18.14), when no export version is configured.

Workaround: There is no workaround.

- CSCsm37058

Symptom: A Cisco 3800 router repeatedly reloads upon boot up.

Conditions: Occurs if the IOS software has got fix for CSCsk32095 and NM-1FE-FX-V2 is installed.

Workaround: None

- CSCsm45113

Symptom: Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

Workaround: Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB. instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Further problem description: The **clear ip route *** command can correct the routing table until the next poll of ipRouteTable MIB.

- CSCsm48415

Symptoms: Cisco Customer Voice Portal (CVP) does not release the port if a user hangs up during database look up.

Conditions: Occurs with the following software configurations: - CVP 3.0 and Cisco IOS Release 12.4.(3g) - CVP 4.1 and Cisco IOS Release 12.4(15)T

Workaround: There is no workaround.

- CSCsm50498

Symptoms: During normal operation of Gateway Load Balancing Protocol (GLBP), when state changes from active to listen, the router stops forwarding traffic destined to the virtual MAC. Router still responds to the interface MAC.

Conditions: Occurs on Cisco 1700 routers running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCsm51299

Symptoms: CSCsl27236 did not catch all of the areas needed to be fixed due to code divergence.

Conditions: The symptoms can be observed under stress conditions and when ipsec-isakmp is enabled.

Workaround: There is no workaround.

- CSCsm55553

Symptoms: A continuous ringback tone is heard at the calling side even after the off-hook of the called side.

Conditions: This symptom is observed on an MGCP endpoint using the LCS package, after the fix for CSCsb28921.

Workaround: Use a Cisco IOS version without the fix for CSCsb28921.

- CSCsm57122

Symptoms: This is an interoperability issue of SSH and SCP among several open SSH clients and the Cisco IOS client.

Conditions: SCP is not working simultaneously with the Putty SSH client and CiscoWorks. When transferring the Cisco IOS image to the device, the CPU is being utilized heavily by the SSH process (noticed through the **show proc cpu** command). Also the file transfer rate is very low at 16 to 20 KB/s.

Workaround: There is no workaround.

- CSCsm62680

Symptoms: Dynamic NAT using a route-map with reversible fails to allow outside-inside traffic when the route-map has a deny statement first.

Conditions: This symptom is observed when the route-map is configured.

Workaround: Remove the route-map deny statement, or use an ACL.

- CSCsm64118

Symptoms: The router may crash when the **no ip dhcp pool word** command is issued from the VTY.

Conditions: This symptom is observed on a Cisco router when the **ip dhcp pool word** command is issued from the console and removed from VTY. Configuring dhcp class (class abcd) in the **ip dhcp pool word** mode, causes the router to crash.

Workaround: There is no workaround.

- CSCsm69147

Symptoms: An H.323 gateway may crash with memory corruption.

Conditions: The symptom is observed on a Cisco platform that functions as an H.323 gateway and that is running Cisco IOS Release 12.4(7e) and 12.4(13e). It may be observed in other releases as well. It occurs whenever the H.323 gateway wants to connect to a remote host and there are no free sockets available for this process.

Workaround: There is no workaround.

- CSCsm70774

Symptoms: The router crashes when a kron policy-list is modified from the console after that kron policy-list has been deleted by another user on a different vty.

Conditions: This symptom can be observed on a Cisco router when the **kron policy-list word** is issued from the console and removed from the VTY. Using the command **cli abcd** in the console, while still in the **kron policy-list word** mode, causes the router to crash.

Workaround. There is no workaround.

- CSCsm83906

Symptoms: After a shutdown of the serial interface, the **no shutdown** command will not restore the interface.

Conditions: This issue is seen on a Cisco 3800 series router installed with a VWIC2-xMFT-G703 card (either onboard slot or HDV2 slot) connected back-to-back with another Cisco 3800 series router with a VWIC2-xMFT-G703 card, that is configured for unframed service.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller, or unplug and replug the E1 cable.

- CSCsm87206

Symptoms: An alternate PVC may go down if you reload the local PE line card 10 seconds after the remote PE line card.

Conditions: This symptom is observed with a Cisco 12000 router that is loaded with a Cisco IOS Release 12.0(32)SY0I image. The local PE is configured with 4xCT3, and the remote PE is configured with 1xSTM1 and L2TPv3.

Workaround: Reload with a long delay between the local and remote PEs LC.

- CSCsm88305

Symptoms: A router running Cisco IOS may crash with a bus error.

Conditions: This is seen on the Cisco 2800 series platform when one or both of the onboard ethernet ports are configured as part of an etherchannel. Under low to medium traffic loads, the device may crash when executing **show run** or **write mem** commands. It also might crash without user intervention under high traffic loads.

Workaround: Do not use the etherchannel feature for onboard ethernet ports on the Cisco 2821.

- CSCsm89475

Symptoms: No output is seen from the **show policy-map interface** command when **service-policy output OUT_WAN** is configured on ATM interfaces when router is receiving QoS traffic from testing device.

Conditions: Observed on a Cisco 3800 series router. May affect other mid-range routers.

Workaround: There is no workaround.

- CSCsm89642

Symptoms: Cisco router may experience bus crash when the **show crypto sessions** command is entered.

Conditions: Occurred on a Cisco 7301 router configured as an VRF-aware IPSEC EzVPN server with clients using RADIUS x-authentication.

Workaround: There is no workaround.

- CSCsm89735

Symptoms: A router might crash when the **show idb** command is issued.

Conditions: The crash is seen when the **show idb** command is issued after a large number of PPPoE sessions (for example, 6000 sessions) are initiated and cleared. The crash is seen with IPv6, but it is not seen with IPv4.

Workaround: There is no workaround.

- CSCsm92206

Symptoms: A router may crash when a range of interfaces is set to default configurations.

Conditions: The crash occurs when a range of interfaces is configured in a console connection to belong to a bridge group and when the same set of configurations is removed simultaneously from a vty connection.

Workaround: Avoid simultaneous tasks (configuring/unconfiguring) through the console and vty.

- CSCsm95129

Symptoms: The **no ip next-hop-self eigrp** command does not work after mutual redistribution with BGP (either iBGP or eBGP).

Conditions: This has been observed on any platform. The combination RIP/EIGRP or OSPF/EIGRP works instead.

Workaround: There is no workaround.

- CSCsm96833

Symptoms: A router may crash when a multicast packet is forwarded on a tunnel interface.

Conditions: This symptom is observed when multicast routing and egress NetFlow are enabled. This is a platform-independent bug.

Workaround: Disable egress NetFlow on the tunnel interface.

- CSCsm99079

Symptoms: The kron process may generate the following syslog and cause the device to reload:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more
than (2000)msecs
(1/0),process = Kron Process.
-Traceback= 0x42725288 0x42725778 0x42724AC0 0x41E0D72C 0x41E0E0BC 0x41E0E3FC
```

Conditions: The symptom is observed when the command **kron** is configured with the *at* parameter.

Workaround: Try redesigning the **kron** command to use the *in* parameter.

- CSCso00792

Symptoms: After receiving disconnect message from ISDN, the actual call disconnection is delayed by 64 seconds.

Conditions: The symptom is observed when the disconnect is received from the incoming ISDN call leg for a TDM-hairpin, DSPless call.

Workaround: There is no workaround.

- CSCso03047

Symptoms: The multilink interfaces stop forwarding traffic, and the serial interfaces out of the multilink start to flap.

Conditions: This symptom is observed when the E3 controller is saturated.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller.

- CSCso04657

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCso05337

Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at the following link

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>

- CSCso05771

Symptoms: When clearing the first entry of local domain lists with similar entries, the router crashes if **show run** is entered.

Conditions: Occurs with routers configured with a domain list similar to this example:

```
ip urlfilter exclusive-domain permit www.cisco112.com
ip urlfilter exclusive-domain permit www.cisco186.com
ip urlfilter exclusive-domain permit www.cisco173.com
ip urlfilter exclusive-domain permit www.cisco21.com
ip urlfilter exclusive-domain permit www.cisco194.com
ip urlfilter exclusive-domain permit www.cisco78.com
ip urlfilter exclusive-domain permit www.cisco124.com
```

If the following command is entered: **no ip urlfilter exclusive-domain permit www.cisco112.com**

The router crashes when **show run** is entered.

Workaround: Do not delete the first entry in similar domain lists.

- CSCso14464

Symptoms: The router may fail to load Cisco IOS Release 12.4(19.8)T and may show the following error message:

```
loadprog: error - program section linked to illegal address
```

Conditions: The symptoms are observed on a Cisco 1800/1810 series, a Cisco 1700 series and a Cisco 815 series router running Cisco IOS Release 12.4(19.8)T.

Workaround: There is no workaround.

Further Problem Description: This is a compiler/link issue.

- CSCso14884

Symptom: Router crashes upon changing interface physical-layer from sync to async on a serial interface while it is in loopback mode.

Conditions: Occurs on Cisco 3800 Series

Workaround: Remove loopback mode before changing physical-layer from sync to async.

- CSCso15151

Symptoms: When Multicast Distributed Fast Switching is configured, a VIP crashes on a Cisco 7500 router that is running a Cisco IOS 12.3 release.

Conditions:

1. The router has around 1000 interfaces/subinterfaces.
2. Distributed multicast is configured.
3. The router is running any Cisco IOS 12.3 release.

Workaround: There is no workaround.

Further Problem Description: In summary, the line card is accessing the memory location that has been freed already. This results in the VIP crashing. There are sanity checks that are missing in Cisco IOS 12.3 releases. The problem is similar to what bug CSCdm29808 does on line cards of the Cisco 12000 Internet series router (this router does not support Cisco IOS Release 12.3). This basically checks if the interface index on MDFS messages is less than the MDFS Idb map size, which indicates the current size of the Idb map table.

- CSCso15220

Symptoms: A Cisco router may experience a memory leak in the VTSP process. The router appears to lose its free memory until it starts to display “SYS-2-MALLOCFAIL” messages in the log and finally crashes per low memory condition.

Conditions: The symptoms occur only when a call fails before it reaches the connect state.

Workaround: The only workaround is to schedule router manual reloads at regular intervals, so that the outages occur at the lowest-impacting moments.

- CSCso19528

Symptoms: Traffic may not flow after a switchover.

Conditions: The symptom may be observed when dLFioLL + HA is configured on a Cisco 7500 router.

Workaround: Wait for standby to come up.

- CSCso22331

Symptoms: A Cisco 2811 router running as voice gateway may crash after enabling the **debug voip vtsp event** command.

Conditions: The symptom can be seen when 2-stage dialing is enabled and SETUP_ACK with a Progress Indicator is received on the outbound leg of the router.

Workaround: Disable the **debug voip vtsp event** command.

- CSCso22730

Symptoms: Prefixes learned via IGP (ISIS) get assigned “imp-null” as the local label for them.

Conditions: The router has ECMP paths to uplink routers via POS interfaces. It runs ISIS as an IGP. There could be TE tunnel configured on the POS interface. And frequent interface flaps.

Workaround: There is no workaround. Clear the route or flap the interface to bring back the correct local label.

- CSCso24243

Symptoms: A VC associated with a VT keeps flapping.

Conditions: This symptom is observed when LFloATM is configured on a Cisco 7200 or when dLFloATM is configured on a Cisco 7500 router.

Workaround: There is no workaround.

- CSCso25559

Symptoms: IKE/IPSec fails to come up.

Conditions: This symptom occurs when two different sub-CAs of a third-party vendor are used as peers.

Workaround: There is no workaround.

- CSCso30073

Symptoms: EIGRP neighbors are not coming up after an IP address change on the interface and the new subnet is added to the EIGRP autonomous system.

Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(20)T.

Workaround: There is no workaround.

- CSCso32831

Symptoms: A Cisco 7200 NPE-G2 router may crash when the command **show usb device / 0A** is entered.

Conditions: The symptoms are observed on a Cisco 7200 NPE-G2 router that is running image c7200p-adventerprisek9-mz.124-19.9.T1.

Workaround: Use the command **show usb device** to list all USB devices.

- CSCso38649

Symptoms: Memory leaks are seen on a SIP-TDM gateway, leading to low available memory. Low memory can cause no access to the console and can also negatively affect normal functionality.

Conditions: This symptom is observed when supplementary services are invoked on a SIP-TDM gateway that is running Cisco IOS Release 12.4(13e).

Workaround: There is no workaround other than reloading the router.

- CSCso41513

Symptoms: When using the **ip helper-address** command to forward directed broadcast, an incomplete ARP entry will be created for the helper-address configured even if it is not a directly connected subnet. This may break BOOTP forwarding to the DHCP server.

Conditions: The symptoms are observed in Cisco IOS Release 12.4(19) only. Cisco IOS Release 12.4(18) does not have this issue.

Workaround: Configure proxy-arp on the next hop device on the path to the DHCP server.

Alternate Workaround: Configure static ARP on the router for the helper-address pointing toward the next hop.

- CSCso47363

Symptoms: A Cisco router may crash when the **no bba-group pppoe word** command is issued from the VTY.

Conditions: This symptom is observed on a Cisco router when the **bba- group pppoe word** command is issued from the console and removed from VTY using the **no bba-group pppoe word** command. In this mode, when giving the command service profile “abcd refresh 2” in the console, the router will crash.

Workaround. There is no workaround.

Further Problem Description: The issue impacts device operations. This is a corner case issue, seen in an unusual sequence of testing. This issue is not seen on Cisco IOS Release 12.4(21).

- CSCso47627

Symptoms: A Cisco router may crash while doing a simultaneous operation in **pvc-in-range 0/32** and **vc-class atm word**.

Conditions: This symptom is observed while configuring simultaneously in **pvc-in-range 0/32** and **vc-class atm word**.

Workaround. There is no workaround.

- CSCso47788

Symptoms: Customer initially running a 6xT1 MLP bundle using three VWIC-2MFT-T1 modules on same slot 0 of a Cisco 3825 router. The Customer is running both voice and data over this MLP link with QoS (LLQ/CBWFQ) applied to the multilink. The MLP circuit is connected to an MPLS network. The customer has fragmentation disabled on the multilink.

The issue occurs when customer adds a 7th and/or 8th T1 to the MLP bundle, which is connected on slot 2 (VWIC2-2MFT-T1/E1). The customer sees increased latency and jitter using extended pings over the MLP bundle.

Conditions: Occurs on a Cisco 3825 running the c3825-sp-servicesk9-mz.124-7b Cisco IOS image and using a VWIC2-2MFT-T1/E1 module installed in slot 2 (NM-HDV2-2T1/E1).

Workaround: Manually configure **tx-ring-limit 2** under serial interfaces residing on the VWIC2-2MFT-T1/E1.

- CSCso53653

Symptoms: A Cisco router may leak memory if configured for an Embedded Event Manager (EEM) applet that utilizes the **action tag cli** command.

Conditions: This occurs under two conditions. Either there is not enough memory for the action to complete properly, in which case there will be memory allocation failure messages sent to the log. Alternatively, there is not enough vtys available to run the action, in which case the following errors may be seen in the log:

```
%HA_EM-3-FMPD_CLI_CONNECT: Unable to establish CLI session: no more tty lines
%HA_EM-3-FMPD_ERROR: Error executing applet appletname statement tag
```

This only occurs in EEM versions 2.2 and earlier. EEM 2.2 is available in Cisco IOS Release 12.4 Mainline. EEM 2.3 and later are not affected.

Workaround: Increase the number of vty's so that the policy will always be able to get one. Do not run the IOS device low on memory.

- CSCso54391

Symptoms: An MLPP call receiving preemption for reuse on unanswered call from the PBX fails to complete.

Conditions: This symptom is observed on all platforms.

Workaround: There is no workaround.

- CSCso63102

Symptoms: Numerous bad enqueue errors on the console resulting in the reload of the Cisco 2800 or Cisco 1800 routers.

Conditions: Occurs when the router has IPsec and GRE configuration with **tunnel route-via Serial0/0/0 mandatory** command on the tunnel interface.

Workaround: Avoid using **tunnel route-via** command.

- CSCso63693

Symptoms: Configuring the **passive-interface default** command in ISIS when existing interfaces exceed 255, or loading/reloading the router when interfaces exceeding 255 exist in the startup-configuration, may generate the following error message: ISIS: Maximum circuit limit (255) has reached. Subsequent interfaces are not advertised into ISIS as expected.

Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(33)SXH1 and where interfaces exceeding the 255 limitation exist in the startup-configuration and the router is loaded/reloaded. It is also observed when interfaces exceeding the 255 limitation are configured after the command **passive-interface default** is used.

Workaround: Use the **passive interface** command to manually configure all interfaces.

- CSCso65623

Symptoms: The allowed VLANs on trunk are only displayed correctly in first two lines of running configuration. For example:

```
show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol	on	802.1q	trunking	1

```
Port      Vlans allowed on trunk
```

```
Pol
1,349,377,408,420,433,492,510,512-513,519,555,573,590-591,603,628,641,647-649,653,656,660,1002-1005
```

The above state is translated to following running-configuration:

```
interface Port-channel1
  switchport trunk allowed vlan 1,349,377,408,420,433,492,510,512,513,1002-1005
  switchport trunk allowed vlan add 519,555,573,590,591,603,628,641,647-649,653
  switchport trunk allowed vlan add 660
  switchport mode trunk
end
```

Conditions: The symptom is observed on a Cisco 3800 series, a 3700 series and a 2800 series router equipped with NM-16ESW and running Cisco IOS Release 12.4 (19).

Workaround: Manually edit the startup-configuration on NVRAM by adding the missing VLAN in the third line. For example:

```
interface Port-channel1
  switchport trunk allowed vlan 1,349,377,408,420,433,492,510,512,513,1002-1005
  switchport trunk allowed vlan add 519,555,573,590,591,603,628,641,647-649,653
  switchport trunk allowed vlan add 656,660
  switchport mode trunk
end
```

- CSCso67601

Symptoms: When a call using a CMM ACT transcoder is disconnected from the H323 endpoint, the transcoder shows as being unregistered. The transcoder remains unregistered on resetting it from the CCMAdmin page. The **show dspfarm all** command shows two active connections even though the CCM side has already cleared the call.

Conditions: The symptoms are observed when a CMM ACT transcoder is used and the call is cleared by an H323 endpoint.

Workaround: On reloading the jagger, the transcoder registers to the CCM.

- CSCso68344

Symptoms: The command **no service dhcp** to stop DHCP server/relay from the router may cause a crash.

Conditions: The symptom is observed when router is receiving requests from DHCP clients at high rate and duplicate-address detection ping is active.

Workaround: There is no workaround.

- CSCso68463

Symptoms: The router may crash when the command **test crash** is executed and then option “S” is selected.

Conditions: The symptom occurs on a Cisco router that is running Cisco IOS Release 12.4(15)T5.

Workaround: There is no workaround

Further Problem description: When the router is configured with the commands **memory record filter exclude <WORD>**, **memory record traceback depth 16 hashbits 12**, **memory record events buffer 1024** and then execute the command **test crash** and select the option “S” from the crash menu, the router crashes.

- CSCso68864

Symptoms: Shape peak percent and absolute value calculations are wrong while attaching policy-map to interface.

Conditions: Occurs when policy-map is attached to interface.

Workaround: There is no workaround.

- CSCso70587

Symptoms: The RTP ports are being opened at H323 and the SSRC for the SRTP call is being updated before the PROCEEDING/ALERTING indication is received on the ISDN end. This may result in a “%DSM-3-INTERNAL” error message.

Conditions: The symptoms are observed on a Cisco 2811 series and an AS5xxx router.

Workaround: Disable the SRTP configuration and initiate normal RTP calls.

- CSCso72893

Symptoms: A warning message may be seen when the encapsulation value changes on an interface with CDP disabled, and c5350-boot-mz image build is failed with the following errors:

```
sub_core_platform.o(.text+0x1a10c): In function `encapsulation_command':
: undefined reference to `cdp_supported_int'
make-3.79.1-p3: *** [c5350-boot-m.czsun] Error 1
sub_core_platform.o(.text+0x1a10c): In function `encapsulation_command':
: undefined reference to `cdp_supported_int'
```

Conditions: The symptom is observed when the encapsulation value is changed on an interface with CDP disabled, followed by CDP enabled.

Workaround: There is no workaround.

Further Problem Description: This is an expected behavior. Warning messages will be seen whenever encapsulation changes with CDP being disabled on the interface. This is due to the commit of CSCso59137.

- CSCso74996

Symptoms: A “%SYS-4-CHUNKMALLOCFAIL” error message is seen. The cause field of the message states “Not a dynamic chunk”.

Conditions: The symptom is observed in conditions where an application depends heavily on chunks.

Workaround: There is no workaround.

Further Problem Description: This issue will not affect the working/operation of the system although it may cause some performance slow down. The message “%SYS-4-CHUNKMALLOCFAIL” with cause field being “Not a dynamic chunk” shows the problem is occurring. An error message “%SYS-4-CHUNKMALLOCFAIL” with a cause field other than “Not a dynamic chunk”, is unrelated to this issue.

- CSCso77729

Symptoms: When trying to load and verify the image c837-k9o3sy6-mz, the following error message is shown:

```
"program section linked to illegal address".
```

Conditions: The symptom is observed on a Cisco 837 router that is running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCso78427

Symptoms: A voice gateway is crashing at ccip_apply_sip_to_pstn_calling_policy with a TLB (store) exception.

Conditions: This symptom is observed on a Cisco AS5400XM that is running either Cisco IOS Release 12.4(19) or Cisco IOS Release 12.3(14)T6.

Workaround: There is no workaround.

- CSCso80215

Symptoms: QOS marking is not placed on SYN packet when marking is applied on outbound interface.

Conditions: The symptom is seen on a Cisco IOS router that is running Cisco IOS Release 12.3 mainline, Release 12.3T, Release 12.4 mainline or Release 12.4T prior to Release 12.4 (4)T. Cisco IOS firewall enabled on inside interface, QOS marking outbound on outside.

Workaround: Any of the following:

1. Disable fast-switching;
2. Remove IOS FW from inside interface; or
3. Mark packets inbound and apply QOS on outbound interface.

- CSCso80288

Symptoms: The value of AOC is missing for the Release Message.

Conditions: The symptom is seen for switch type basic-net3. It occurs when configuring OGW and TGW with the **isdn global-disconnect** command.

Workaround: There is no workaround.

- CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.

This security advisory is being published simultaneously with announcements from other affected organizations.

- CSCso84235

Symptoms: A wide variety of data path failures are seen, including tracebacks, crashes, and up to 99% packet loss for crypto-protected tunnel interfaces.

Conditions: While the issues were reported for a Cisco 7200 series router and a Cisco 7301 router, the issue is not restricted to just those platforms. The conditions vary, and can include updating the crypto configuration, or simply passing traffic that the router needs to encrypt.

Workaround: No workaround has been verified.

- CSCso91078

Symptoms: A Cisco IAD2430 may reload unexpectedly due to a bus error (Sig=10).

Conditions: The symptom is seen on a Cisco IAD2430 that is running Cisco IOS Release 12.4(15)T4.

Workaround: There is no workaround.

- CSCso91230

Symptoms: A router may display the following error:

```
%LINK-2-INTVULN: In critical region with interrupt level=0, intf=ATM0
-Process= "IGMP Snooping Receiving Process"
```

Conditions: The symptom is observed when bridged traffic is passing to an MLPP interface.

Workaround: Disable IGMP snooping with the **no ip igmp snooping** command.

- CSCso98389

Symptoms: The **initiate-to** command is being rejected under the “config-vpbn-req-out” mode.

Conditions: The symptom is seen in Cisco IOS Interim Release 12.4(19.16)T1.

Workaround: There is no workaround.

- CSCsq02771

Symptoms: DHCP relay may hang when request for IP address is received from a DHCP client on an unnumbered in an MPLS and VPN setup.

Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(19.16)T1.

Workaround: There is no workaround.

- CSCsq11750

Symptoms: A Cisco router may crash when the **no mgcp** and the **no mgcp profile profile-name** commands are issued from the VTY, and the command **call-agent ip-address** is configured through the console in “config- mgcp-profile” mode.

Conditions: The symptom is observed when there is simultaneous operation between the console line and the VTY line.

Workaround: Configure using a single telnet connection instead of two.

- CSCsq13348

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>.

- CSCsq20970

Symptoms: On the Cisco 2432 platform UUT, the “atm” option is missing in the “mode” CLI when the T1 controller is being configured for ATM.

Conditions: The symptom is observed on the Cisco 2432 platform with a T1 controller.

Workaround: There is no workaround.

- CSCsq28593

Symptoms: There may be a CMM build failure on Cisco IOS Release 12.4 mainline.

Conditions: The symptom is observed when building CMM platform images on Cisco IOS Release 12.4 mainline.

Workaround: There is no workaround.

- CSCsq74300

Symptoms: Loopbacks, Null0 and other non Point-to-Point interfaces are not allowed in a route-map set command due to the changes introduced with caveat CSCsk63775.

Conditions: This issue is seen with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsr16693

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>.

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Resolved Caveats—Cisco IOS Release 12.4(19b)

Cisco IOS Release 12.4(19b) is a rebuild release for Cisco IOS Release 12.4(19). The caveats in this section are resolved in Cisco IOS Release 12.4(19b) but may be open in previous Cisco IOS releases.

- CSCsm80048

Symptoms: Policy on MFR interface stays in suspend mode after a **shut/no shut** even though required bandwidth is available.

Conditions: This symptom occurs with a QoS policy attached to MFR interface on a Cisco 7500 router.

Workaround: There is no workaround.

- CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.

This security advisory is being published simultaneously with announcements from other affected organizations.

Resolved Caveats—Cisco IOS Release 12.4(19a)

Cisco IOS Release 12.4(19a) is a rebuild release for Cisco IOS Release 12.4(19). The caveats in this section are resolved in Cisco IOS Release 12.4(19a) but may be open in previous Cisco IOS releases.

- CSCek78237

Symptoms: A short CPU hog seen in the ATM PA Helper process when an interface flaps and the framing configuration is modified on the interface.

Conditions: This symptom is observed on a Cisco 7200 with a PA-A3-T3 adapter that is running Cisco IOS Release 12.2(25)S or 12.2(31)SB (and possibly other Cisco IOS releases).

Workaround: There is no workaround.

Further Problem Description: The CPU hog is enough to cause OSPF adjacencies (with fast hello) to go down on other unrelated interfaces. The same problem is seen if BFD is configured.

- CSCsl04516

Symptoms: A Cisco router may experience the following errors:

```
Jan 11 07:06:58: %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x476292F0 -Process= "Skinny
Socket Server", ipl= 0, pid= 260 -Traceback= 0x41259724 0x41A50418 0x41A54754
0x41A28134 0x41A2AFA4 0x41A2F30C 0x4095AB80 0x4095B5F4 0x423CD6E4 0x423CD6C8
```

```
Jan 11 07:06:58: %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x476292F0 -Process= "Skinny
Socket Server", ipl= 0, pid= 260 -Traceback= 0x41259724 0x41A50418 0x41A54754
0x41A28134 0x41A2AF24 0x41A2F30C 0x4095ABA4 0x4095B5F4 0x423CD6E4 0x423CD6C8
```

Phones that are running over secure channels will have registration problems.

Conditions: This symptom occurs on a Cisco 2821 router that is running Cisco IOS Release 12.4(18).

Workaround: There is no workaround.

- CSCsl10459

Symptoms: Routers that are running Cisco IOS Release 12.4(13b) and Release 12.4(16) may crash when the **show crypto pki timers** command is executed.

Conditions: This symptom is observed under a narrow set of conditions. Offending conditions occur when certificates are issued Certificate Distribution Point formatted in URL format. Certain other unknown circumstances must also occur.

Workaround: Avoid using the **show crypto pki timers** command.

- CSCsl78850

Symptoms: When the WAN is restored between an MGCP/SRST gateway and CallManager, the MGCP gateway intermittently fails to register back with CallManager.

Conditions: Connectivity to the CallManager from the gateway is stopped. When the gateway goes in SRST, a PSTN call is placed to a phone that registers with the gateway. WAN connectivity is then restored. MGCP has one primary call agent and two redundant hosts configured.

Workaround: Reload the gateway.

Further Problem Description: When the gateway is in this “stuck” state of not registering with the CallManager, if “no ccm-manager mgcp” is configured, it does not take effect, and “no ccm-manager redundant-host ...” also does not take effect. The following error message is displayed:

```
cmapp_service_emptying_redun_hostlist: Error: cannot execute CCM host change -- must
configure again!
```

- CSCsm55553

Symptoms: A continuous ringback tone is heard at the calling side even after the off-hook of the called side.

Conditions: This symptom is observed on an MGCP endpoint using the LCS package, after the fix for CSCsb28921.

Workaround: Use a Cisco IOS version without the fix for CSCsb28921.

- CSCsm57122

Symptoms: This is an interoperability issue of SSH and SCP among several open SSH clients and the Cisco IOS client.

Conditions: SCP is not working simultaneously with the Putty SSH client and CiscoWorks. When transferring the Cisco IOS image to the device, the CPU is being utilized heavily by the SSH process (noticed through the **show proc cpu** command). Also the file transfer rate is very low at 16 to 20 KB/s.

Workaround: There is no workaround.

- CSCso41513

Symptoms: When using the **ip helper-address** command to forward directed broadcast, an incomplete ARP entry will be created for the helper-address configured even if it is not a directly connected subnet. This may break BOOTP forwarding to the DHCP server.

Conditions: The symptoms are observed in Cisco IOS Release 12.4(19) only. Cisco IOS Release 12.4(18) does not have this issue.

Workaround: Configure proxy-arp on the next hop device on the path to the DHCP server.

Alternate Workaround: Configure static ARP on the router for the helper-address pointing toward the next hop.

- CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.

This security advisory is being published simultaneously with announcements from other affected organizations.

- CSCsq13348

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>.

- CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsr16693

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPsec NAT traversal (NAT-T) feature can be used as an alternative.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>.

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Resolved Caveats—Cisco IOS Release 12.4(19)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(19). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(19). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCec10091

Symptoms: A Catalyst 6500 MSFC configured for DHCP forwarding may forward DHCP requests with incorrect source address.

Conditions: This symptom is observed on a Catalyst 6500 MSFC running Cisco IOS image named c6msfc-jsv-mz.121-11b.E. However, this is a platform independent bug.

Workaround: Enter configuration mode and enter the following commands: **no service dhcp service dhcp**

- CSCej49366

Symptoms: If a default metric and a redistribution metric are configured under EIGRP, the redistributed routes are sometimes removed from the EIGRP topology table. Occurs with the following configuration:

```
router eigrp 1
 redistribute ospf 100 metric 1544 10 255 1 1000
 network 1.0.0.0
 network 4.0.0.0
 default-metric 100 100 100 100 100
 auto-summary
 eigrp event-logging
```

Conditions: Occurs after the default metric statement is removed.

Workaround: Add the default metric statement back into the configuration, or remove and re-apply the explicit redistribute statement for the donor protocol (OSPF in the above example).

- CSCek75633

Symptoms: A router may crash resulting in service impact.

Conditions: This symptom is observed on a 7200 router with NPEG2 when you attach a VC class to an ATM bundle. This is platform-independent. On other platforms a crash will not occur only traceback errors are noticed

Workaround: There is no workaround.

- CSCek76062

Symptoms: A router crashes because of a block overrun (overwriting the memory block).

Conditions: This symptom is observed only when templates are exported in the export pack, which is used only in version 9 version of exporting.

Workaround: Version 5 could be used for exporting.

- CSCsa65314

Symptoms: Inbound calls on a MGCP controlled CAS trunk may experience symptoms where the call does not complete and the calling party hears dead air. When this occurs, it will be experienced at that particular timeslot on the digital trunk until some manual intervention take place to correct this.

Conditions: This has been found to occur at times on Cisco IOS VoIP gateways with CAS trunks configured from MGCP back to Cisco Unified CallManager (CUCM/CCM). An inbound call on a timeslot that is in this state will show the vtsp state in **show voice call summary** as S_DIGIT_COLLECT and will not progress past this point.

Once source of this issue has been when the status of the timeslot on the CallManager and the gateway are not the same. For example, the CallManager may indicate that the channel is out of service (OOS) while the gateway has the status of this timeslot as in-service (idle). Please refer to CSCef58219 which has seen to lead to this state. If this issue is being seen because of this difference in status between the CallManager and the IOS gateway, the recommended action is to upgrade the CallManager with a release that contains the fix for CSCef58219.

Workaround: The only known workaround to prevent this issue from occurring is to use H323 instead of MGCP with CAS trunks.

Once in this state, to recover the timeslots you can: 1. Enter the **shutdown** command and the **no shutdown** command on the voice port. 2. When there are multiple channels stuck enter **no mgcp** and then **mgcp**.

- CSCsg16778

Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

Workaround: There is no workaround.

Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- CSCsg64163

Symptoms: Cisco IOS does not handle packet fragments for port specific NAT rules like:

```
ip nat inside source static udp 192.168.21.2 500 interface FastEthernet0/0 500
ip nat inside source static udp 192.168.21.2 4500 interface FastEthernet0/0 4500
```

Only first fragment is being translated, others are not. This symptom remains even if the ip virtual-reassembly command is active on interfaces.

Conditions: This symptom has been observed on Cisco IOS Release 12.4 and Release 12.4T.

Workaround: There is no workaround.

- CSCsh22725

Symptoms: Outbound calls fail on a MGCP-controlled CAS channel on a Cisco VoIP gateway.

Conditions: This symptom is observed when the following conditions occur:

- A timeslot on an E&M T1 trunk is taken out of service from the connected switch side, showing as a permanent inbound seizure. In this situation, the output of the **show voice call summary** command indicates that the status for this channel is "EM_PARK".
- A Cisco CallManager that interworks with the Cisco VoIP gateway checks the status of the trunk via an MGCP AUEP command. The gateway responds with an "ES: rlc" message, which indicates that the trunk is available for calls.

Because the reported availability and actual availability of the channel are mismatched, all outbound calls on the channel fail.

Workaround: Attempt to clear the out-of-service state from the connected switch side. If this is not possible, when interworking with the Cisco CallManager, first enter the **shutdown** command followed by the **no shutdown** command on the voice port and then enter the same commands on the T1 controller. Doing so causes the gateway to send an NTFY message that indicates that there is an inbound seizure on the channel.

- CSCsi06948

Symptoms: A switch or router may crash because of a bus error after a BGP dampening-related command is entered. Occurs when the **sh ip bgp dampening dampened-path** command is entered while the neighbor is being cleared.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF7 but may also affect other platforms and releases.

Workaround: There is no workaround.

- CSCsi20225

Symptoms: Continuous tracebacks may be generated on an LNS.

Conditions: This symptom is observed when you bring up PPPoX or L2TP sessions over multiple tunnels without traffic being processed over these sessions.

Workaround: There is no workaround.

- CSCsi68963

Symptoms: Cisco 7200P router crashes while removing IPv6 Protocol Independent Multicast (PIM) bootstrap router (BSR) candidate from configuration.

Conditions: This happens when unconfiguring IPv6 PIM BSR candidate.

Workaround: There is no workaround.

Further Problem Description: After RP information is learned on all of the routers, delete the ACL first, then the BSR candidate.

- CSCsi73481

Symptoms: PPPoE sessions may fail to establish on IDBless/ambiguous VLAN.

Conditions: PPPoE sessions served on a VLAN not associated with an ethernet subinterface may fail to come up because PPP packets are being sent without an 802.1Q header. This only happens when there is no subinterface configured with the native 802.1Q VLAN.

Workaround: A workaround is to configure a subinterface with the native VLAN.

- CSCsj46178

Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router in either global MGCP configuration or MGCP profile.

Workaround: Do not configure the **endpoint naming t3** command. Use T1 endpoint naming instead.

- CSCsj49255

Symptoms: If there is an ACL and DSCP being used for packet matching on class- map, only the first packet descriptor will get a match, and everything else will not. If DSCP is removed, the packet matching works again.

Conditions: This symptom is observed on a Cisco 7200 with ACL and DSCP with match all option.

Workaround: There is no workaround.

- CSCsj59278

Symptoms: When a label switch controller (LSC) for a BPX has an MPLS binding for an IP route, and that IP route goes away, it will correctly get a binding for a less specific IP route, assuming one exists. The problem occurs when that more specific IP route returns. The MPLS bindings stays with the less specific route, instead of switching to the more specific route.

Conditions: Occurs on Cisco IOS Release 12.4(13a). When an LSC has two routes, the more specific route must be removed, then re-added for this problem to occur.

Workaround: Clear the IP route for both routes to correct the problem.

- CSCsj74102

Symptoms: DTMF digits are not recognized by the remote side.

Conditions: Occurs on a Cisco MGW using MGCP configured for DTMF RFC2833 standard under control of Cisco PGW2200. When the first digit is pressed it contains a wrong synchronization source identifier in an RTP header.

Workaround: There is no workaround.

- CSCsj74812

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: Occurs when running **show** commands on an exec session that has been established through one of the integrated modems on a WIC-AM or WIC-2AM. This is only seen on async cards with gt96k, hwic or pquicc drivers.

Workaround: There is no workaround.

- CSCsj89544

Symptoms: If a BGP keepalive message fails to be sent to a BGP peer because the transport link is down, the neighbor BGP peer does not accept any further keepalive packets even though TCP retransmits the failed message using a backup path. This eventually causes the BGP peer to go down because of holdtime expiration.

Conditions: This happens when TCP retransmissions occur on MPLS-enabled network. This is seen only when MPLS is configured on Catalyst 6500 or Cisco 7600.

Workaround: There is no workaround.

- CSCsj93012

Symptoms: A Cisco 7500 router may crash when QoS is enabled.

Conditions: Occurs when ATM and serial interfaces have QoS configurations as output/input policy and when peer is reloaded.

Workaround: There is no workaround.

- CSCsk25651

Symptoms: With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM)/CallManager and utilizing SRST functionality, when the IP phones are registered to the SRST router, the message-waiting indication (MWI) states may be incorrect.

Conditions: When a phone registers to a Cisco SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come, first-served fashion. The MWI state, however, is remembered from the previous registration that used that ephone-dn number so the MWI status could be incorrect.

Workaround: Configure both the SRST router and the CUE to use SUBSCRIBE/NOTIFY MWI method.

- CSCsk26774

Symptoms: Native VLAN information is not included in CDP packets going out ports of an EtherSwitch (ESW) module in Cisco 28xx and Cisco 38xx routers. All the platforms using switchports (of any kind built-in/NM/WIC/HWIC) have this issue: Cisco 8xx, Cisco 17xx, Cisco 18xx, Cisco 26xx, Cisco 36xx, Cisco 37xx, Cisco 28xx, and Cisco 38xx.

Conditions: This symptom causes Cisco IP phone models 7961, 7941 and 7970 that are running SCCP firmware to fail to forward traffic coming from a PC connected at the back of the phone.

Workaround: Enable the "Voice VLAN Access" setting on the phone.

- CSCsk27147

Symptoms: The following SNMP is incorrectly generated:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
```

This issue is affecting the CISCO-MEMORYPOOL-MIB instead.

Conditions: Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

Workaround: Exclude ciscoMemoryPoolMIB from your query with the following commands:
snmp-server view public-view iso included snmp-server view public-view ciscoMemoryPoolMIB excluded Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

- CSCsk35970

Symptoms: Excessive CPU usage occurs on a Cisco 12000 Series Router running Cisco IOS Release 12.0(32)S and configured for BGP multipath with several iBGP and eBGP peers.

Conditions: TblVer is incrementing every 5 minutes, causing the BGP router process to use maximum CPU every 5 minutes.

Workaround: There is no workaround.

- CSCsk42985

Symptom: On a 1841/WIC-1/WIC-1B-U-V2/c1841-adventerprisek9-mz.124-13c combo [hereafter UUT], 180s after BRI interface successfully dials HUB PRI, 1/2 PING packets FAIL from HUB routers destined through UUT to a device on FastEthernet of the UUT, through the CEF switching path.

180 seconds after the ISDN Call from UUT successfully dials HUB PRI, "show adj vi1 internal" changed from point2point(21) to point2point(20) (incomplete) which coincides exactly with the PING failure. It also coincides with the CEF refresh timer triggering.

The direction of the failure is UUT-->HUB router with packets being dropped as "encapsulation failed" in "show ip traffic".

Conditions: Issue has been reproduced on Cisco 1841/WIC-1/WIC-1B-U-V2 using legacy DDR on BRI interface. Issue also reproducible in Cisco IOS Release 124-16.14.

Issue is not reproducible on 1720/WIC-1B-U/c1700-sy-mz.122-40 combo.

Workaround: Disable CEF switching by configuring the **no ip route-cache cef** command on BRI0/1/0 and Fa0/1 on "nhtest2".

- CSCsk54153

Symptoms: A Cisco router may reload unexpectedly with a software forced crash.

Conditions: This symptom is observed when the FXS port is configured with a DN and the gateway is being reset by CallManager 4.2.

Workaround: There is no workaround.

- CSCsk62922

Symptoms: Three-way calls placed from an analog phone connected to a Cisco gateway (configured as an MGCP gateway) may not cut-through audio properly.

Conditions: Observed when using third party device as the MGCP server.

Workaround: There is no workaround.

- CSCsk65601

Symptoms: PPP tunnel does not come up after PE edge interface flapped.

Conditions: This symptom is observed on a Cisco router when the **show mpls l2transport vc** command is entered.

Workaround: Use the **xconnect** command to unconfigure and then reconfigure the xconnect under the serial interface being flapped to restore.

- CSCsk67111

Symptoms: Watchdog timeout seen after switchover.

Conditions: Occurs when high availability RPR mode is configured on a Cisco 7500 router.

Workaround: There is no workaround.

- CSCsk68320

Symptoms: Switch aborts or reloads after the **no ip routing** is entered.

Conditions: Occurs when a Supervisor Engine IV is configured with a minimal IP multicast and Multicast Source Discovery Protocol (MSDP) configuration.

Workaround: There is no workaround.

- CSCsk69533

Symptoms: Card type configuration is lost on a Cisco 7500 router.

Conditions: Occurs when dLFioLL+SSO is configured on a Cisco 7500 and a controller is shutdown followed by a switchover.

Workaround: Reload the router.

- CSCsk78725

Symptoms: While giving T1 controller configuration, the router crashes. This happens on the 8-port multichannel T1/E1 8PRI PA (PA-MC-8TE1+).

Conditions: Occurs on a router running Cisco IOS Release 12.4(17.7) and Cisco IOS Release 12.4(17.4)T1.

Workaround: There is no workaround.

- CSCsk83480

Symptoms: The multilink interfaces are going down while running LFioFR.

Conditions: This symptom is seen when configuring LFioFR. Verify everything is working fine and follow these steps:

```
no encap frame-relay, on the interface
encap frame-relay, on the interface
configure LFioFR DLCI, on the subinterface
default all configs under virtual-template
no int virtual-template 1
int virtual-template 1
configure back all configurations under virtual-template
```

Workaround: There is no workaround.

- CSCsk88637

Symptoms: OAM cells are not generated when a new ATM subinterface and PVC is configured. Check subinterface and PVC status and enable the **debug atm oam interface atm x/x.xxx** command. Subinterface will be up/up. PVC will be down, and no debug output will be seen.

Conditions: This symptom has been seen in various Cisco IOS 12.4 images.

Workaround: Perform **shut/no shut** commands on ATM subinterface.

- CSCsk94179

Symptoms: When IPv6 prefix delegation (PD) assigns a prefix for virtual access, it create a static route for the prefix in the routing table. However, sometimes it creates incorrect static route for the prefix.

Conditions: The problem is observed when IPv6 PD is configured as a L2TP LNS.

Workaround: There is no workaround.

- CSCsk97130

Symptoms: VXML application causes memory leak

Conditions: If the calling document and called document of a subdialog share the same root document, the tree structure used for the root document will not be released after the call session is finished.

Workaround: There is no workaround.

- CSCsk97261

Symptoms: Router crashes with an Unexpected exception to CPU vector traceback.

Conditions:

Issuing the modemui command with a large input parameter in the [modem-commands], such as:

```

host>modemui ATZaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
OK
OK
OK
Host:
00:05:30 UTC Mon Mar 1 1993: Unexpected exception to CPUvector 1200, PC = 804829C4
-Traceback= 804829C4 8049E4B0 8049E798 80492924 803CAE9C 803CB7E0 803CB6D8 803CDE88
80574D04 805759 78 803A6CC8 80CA1B60 80CA2008 80CA21FC 80CA21FC
More information about the Cisco Modem User Interface feature is available at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\_feature\_
guide09186a0080087bf9.html

```

Workaround: There is no workaround.

- CSCsk97384

Symptoms: Abnormally large FreshTime value appears in IVR HTTP client cache entry.

Conditions: This symptom is observed when a VXML voice browser downloads a file from an HTTP server. If the file was modified very recently, the FreshTime for that file may show up with a very large value.

Workaround: There is no workaround.

- CSCsl02927

Symptoms: With no traffic on a PA-A6-OC3SMi card, the max ICMP pings times are seen at 352 ms to 384 ms when testing to an ATM loopback diag. Min/avg are 1/4. This is seen with 1500-byte packets.

Conditions: This symptom is observed with a 7206vxx backplane version 2.8- 2.11 with the PA-A6-OC3SMi ATM card.

Workaround: There is no workaround.

Further Problem Description: This symptom is not observed with version 2.8- 2.11 with the PA-A3-T3 card.

- CSCsl13216

Symptoms: Warm upgrade does not work as expected.

Conditions: Occurs when you perform a warm upgrade from a small IOS image to a large image.

Workaround: Use the **reload** command instead of the **reload warm fileimage-path** command to boot the new image.

- CSCsl14635

Symptoms: T38 negotiation is failing for an incoming UPDATE request that has a T38 offer.

Conditions: This symptom occurs when the voice gateway is running Cisco IOS Release 12.4(15)T and is processing incoming Session Initiation Protocol (SIP) calls. When the SIP call is active and an UPDATE request is received that contains a T38 offer, the UPDAE request is rejected. The switchover from voice to fax fails.

Workaround: Fax over T38 works fine when midcall INVITE is used for T38 negotiation.

- CSCsl18054

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: Occurs on a router running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCsl21123
Symptoms: Entering the **dir stby-harddisk:** command causes the active RP to crash.
Conditions: Occurs on a Cisco 7600 router.
Workaround: There is no workaround.
- CSCsl24858
Symptoms: Cisco 7200 router with PA-VXC/B may go into "hang" state and fail to respond to console.
Conditions: Occurs on a Cisco 7200 router with PA-VXC/B and configured for active calls over the PA.
Workaround: There is no workaround.
- CSCsl25590
Symptoms: The **ip nat inside source route-map rmap7 interface Ethernet1/0 reversible** is not seen in running configuration after reload.
Conditions: Occurs on a Cisco router running Cisco IOS Release 12.4(17.10b).
Workaround: There is no workaround.
- CSCsl25732
Symptoms: GPRS tunneling protocol (GTPv1) interim accounting not sent out when periodic interval is configured.
Conditions: Occured when using a GTPv1 PDP and interim accounting configured for 15 minutes. No interim accounting request was sent out even after 50 minutes. Interim accounting records were not generating at an approximate interval of +/-15 seconds.
Workaround: There is no workaround.
Further Problem Description: Impact is minimal . If timer is configured for 90 seconds, then update should occur at approximately 75 seconds. If the interval is around 50 seconds, the frequency of updates increases.
- CSCsl30214
Symptoms: Router reloads while configuring the **ssg vc-service-map** command.
Conditions: Occurs on a Cisco 7200 series router running Cisco IOS Release 12.4(18.4)T.
Workaround: There is no workaround.
- CSCsl32308
Symptoms: A voice gateway may modify the Presentation Indicator field when processing a voice call.
Conditions: The voice gateway is running Cisco IOS Release 12.4(9)T5 and processing incoming Session Initiation Protocol (SIP) calls. An incoming SIP call that has its Presentation Indicator (PI) field Oct 3a set to 0xA0 or to any other value is changed to 0x00 for no apparent reason when it is forwarded to the Telephony call leg.
Workaround: There is no workaround.
- CSCsl32408
Symptoms: SIP gateway does not pass privacy information to the ISDN leg.

Conditions: The voice gateway is running Cisco IOS Release 12.4(15)T and processing incoming session initiation protocol (SIP) calls. When a SIP message is received on the voice gateway with calling number containing non-digit (calling number preceded by a '+'), then octet_3a information present in the SIP message is not passed to the ISDN leg.

Workaround: There is no workaround.

- CSCs134303

Symptoms: Cisco 7200 router crashes when unconfiguring service policy from Multilink Frame Relay (MFR) interface.

Conditions: Occurs if one of the MFR bundle link interfaces was previously being used for Multilink PPP over Frame-relay. Changing the encapsulation may not clean up queuing configuration properly - a dual first in first out (FIFO) queue may remain on the interface.

Workaround: Ensure a dual FIFO queue is not present on MFR bundle link interface. It should be plain FIFO queue. If it is a dual FIFO, change the interface to HDLC encapsulation, which should remove the dual FIFO queue, then back to MFR bundle link encapsulation.

- CSCs139130

Symptoms: Spurious memory access is seen while establishing L2TP tunnel (PPPoE-relay). The tunnel is never established.

Conditions: Occurs on routers running Cisco IOS Release 12.4(18.2)PI1 when configuring L2TP active discovery relay for PPPoE and establishing PPPoE sessions from client.

Workaround: There is no workaround.

- CSCs143394

Symptoms: Standby RSP reloads and has problems syncing configuration when DS1 controller is removed from DS3 configuration.

Conditions: This problem is seen when SSH is enabled on the router and DS1 controller is added or deleted from the configuration.

Workaround: There is no workaround.

- CSCs154748

Symptoms: DHCPv6 bindings for multiple clients are stored in a virtual-access interface when each different user has the same DHCP Unique Identifier (DUID).

Condition: This problem is observed when a router is configured for PPPoE or L2TP LNS and is working as DHCPv6 prefix delegation (PD).

Workaround: There is no workaround.

- CSCs161164

Symptoms: Router may crash @ipflow_fill_data_in_flowset when changing flow version.

Conditions: Occurs when netflow is running with data export occurring while manually changing the flow-export version configuration from version 9 to version 5 and back to version 9 again.

Workaround: Do not change the netflow flow version while the router is exporting data and routing traffic.

- CSCs162609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsl65407

Symptoms: A routing loop was formed in MPLS/VPN network topology with EIGRP as the PE-CE routing protocol.

Conditions: A receiving Provider Edge (PE) router does not update the EIGRP topology entry for a prefix to match the metric information advertised in the BGP ext.community attribute from the neighboring PE router. EIGRP is ignoring the metric information within the BGP ext. community attribute and opting to use the metric defined within the **redistribute bgp AS metric k1 k2 k3 k4 k5** command.

Workaround: As a temporary solution, modify the **redistribute bgp AS metric k1 k2 k3 k4 k5 command to redistribute bgp AS** and then add a **default-metric k1 k2 k3 k4 k5** command. Clearing the routing table of the PE may also be necessary.

- CSCsl67527

Symptoms: HTML pages inside a TAR file fail to load. This affects web applications such as Security Device Manager (SDM). If SDM is installed in router's flash, user is unable to invoke the HTML page archived inside the TAR. SDM application fails to launch and user will be receive a "page not found" error.

Conditions: Only occurs when files are contained in a TAR file. All other html files can be loaded successfully. For the Cisco IOS Release 12.4 train, the problem was introduced in Cisco IOS Release 12.4(17.6) and fixed in Cisco IOS Release 12.4(18.11).

Workaround: There is no workaround.

- CSCsl67783

Symptoms: On certain router platforms, if multiple subinterfaces are configured on a Fast Ethernet interface and if these subinterfaces are configured for Hot Standby Routing Protocol (HSRP) and the same Virtual MAC address (VMAC), then whenever the router becomes HSRP standby for at least one of these subinterfaces, the router drops all traffic that is directed to the same VMAC on other subinterfaces.

The following is a sample configuration that would be exposed to this issue:

```
interface FastEthernet2/0.4
encapsulation dot1Q 4
ip address 192.168.12.2 255.255.255.0
standby 102 ip 192.168.12.254
standby 102 priority 210
standby 102 preempt
standby 102 mac-address 0200.0000.7700

interface FastEthernet2/0.5
encapsulation dot1Q 5
ip address 192.168.13.2 255.255.255.0
standby 2 ip 192.168.13.254
standby 2 priority 210
standby 2 preempt
standby 2 mac-address 0200.0000.7700 !
```

Conditions: This symptom is observed on Cisco 7200/NPE-400 platform on the motherboard and Fast Ethernet port adapters.

Workaround: The problem does not occur if different VMAC addresses are configured on different subinterfaces or if static VMACs are not used. If the problem is encountered in a production environment, a quick workaround is to shut down the Fast Ethernet interface of the other router in order to make one router HSRP active in all VLANs.

- CSCs168776

Symptoms: When two Cisco transcoders are connected back-to-back, calls may not be properly torn down when the Cisco Unified CallManager (CCM) goes into Call Preservation mode by sending the transcoder a "StartMediaFailureDetection" message. This can lead to stuck calls until the Skinny Call Control Protocol (SCCP) application is reset or the router is reloaded.

Conditions: Occurs because the transcoder will only send MediaFailure when both RTP streams stop receiving packets for the configured time (default 1200 seconds). If one side continues to receive RTP, MediaFailure will never be sent to CCM.

Workaround: Reset the SCCP application on router or reload the router.

- CSCs170143

Symptoms: Under heavy traffic, ISDN calls may be rejected due to high CPU usage with the following messages seen in the log (with tracebacks):

```
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (98/100). Call
(callID=23524) is rejected.
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (32/18),process
= ISDN.
```

Conditions: This problem occurs only under heavy traffic.

Workaround: There is no workaround.

- CSCs170722

Symptoms: A router running Cisco IOS may crash due to watchdog timeout.

Conditions: Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon mib for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

Workaround: There is no workaround.

- CSCs172281

Symptoms: After a Cisco 7600 series router reloads, host routes created by DHCP relay process for DHCP clients that are connected to unnumbered VLAN interfaces point to wrong VLAN interface.

Conditions: This symptom occurs when interface-index value parameter on the router changes after the router reloads. This parameter is stored in DHCP bindings database on TFTP or FTP server. It is recalculated in case of the router reloading and may change if a new interface is added or existing interface is removed from the configuration. For example, a single interface VLAN is added to the configuration prior to the router reloading.

Workaround: There is no workaround.

- CSCs174712

Symptoms: When an existing Virtual Router Redundancy Protocol (VRRP) tracking entry is re-entered into the configuration of the active RP, the standby RP automatically resets.

Conditions: This problem only occurs after the following sequence of configuration events:

- VRRP is configured to track an existing tracking object.

- The existing tracking object is removed from the global tracking configuration.
- The standby is initiated and establishes the full STANDBY state.
- The user re-enters the VRRP command to track the previously removed tracking object.
- At this point the Standby RP will reset due to PRC mismatch.

Workaround: During normal configuration it is unlikely that the above scenario will be repeated. Crucially the workaround for this defect is to make sure that when VRRP is using a tracked object, the global tracking config for that object must exist at all times. The global tracking config for that object can be removed as long as the tracking entry in VRRP is removed first.

- CSCsl79588

Symptoms: Router running Cisco IOS may crash with a bus error.

Conditions: Occurs when a Cisco router is configured to stream music on hold (MoH) from a .wav file with a header longer than 256 bytes.

Workaround: Do not use .wav files for MoH. Use only .au files.

- CSCsl87400

Symptoms: H323 setup message is malformed after NAT translation

Conditions: Setup message includes the neededFeatures, desiredFeatures, supportedFeatures extensions.

Workaround: Do not use the extensions listed above.

- CSCsl94410

Symptoms: CPU hog condition occurs because of stressful BGP configuration.

Conditions: Occurs in Cisco IOS releases in which CSCsl94410 has been fixed.

Workaround: There is no workaround.

- CSCsm12247

Symptoms: A Cisco IOS router configured for WCCP may stop redirecting traffic following a change in topology.

Conditions: The router must be configured for WCCP redirection using the hash assignment method. When there is only a single appliance in the service group, the loss of hash assignment details is permanent. However with multiple appliances in the group, the loss of assignment information is transitory; the router soon recovers.

Workaround: To recover the assignment details, the WCCP configuration needs to be removed and re-added to the router. Use the **no ip wccp service** command followed by **ip wccp service args** command.

- CSCsm20351

Symptoms: AAL2 trunk alarm is not generated for a resource availability indication (RAI) condition when a T1 is disconnected from a VWIC module.

Conditions: This issue is seen when AAL2 trunking is configured on a Cisco 2811 running Cisco IOS Release 12.4(17a)

Workaround: There is no workaround.

Further Problem Description: This issue is not seen on non-ISR platforms running Cisco IOS Release 12.3.

- CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>

- CSCsm27726

Symptoms: After overwriting DHCP pool and client pool, status of client is IDLE.

Conditions: Occurs on Cisco routers running a pre-release version of Cisco IOS Release 12.4(17b).

Workaround: There is no workaround.

- CSCsm34361

Symptoms: TCP ports may not show open as required during port scanning using NMAP.

Conditions: Occurs on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsm45113

Symptoms: Router may install duplicate routes or incorrect route netmask into route table. It could happen on any routing protocol. The problem is introduced by CSCsj50773. See the Integrated-in field of CSCsj50773 for affected images.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The **clear ip route *** command can restore the route table until next polling of ipRouteTable MIB.

Workaround: Do not poll ipRouteTable MIB. Instead poll newer replacement MIB, ipForward MIB. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Resolved Caveats—Cisco IOS Release 12.4(18e)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(18e). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(18e). This section describes severity 1 and 2 caveats and select severity 3 caveats.

IP Routing Protocols

- CSCek77424

Symptoms: A Cisco router that is running Cisco IOS Release 12.4(13b) might unexpectedly reload with a bus error.

Conditions: This symptom happens during normal operation with NAT configured.

Workaround: There is no workaround.

- CSCsb63652

Symptoms: BGP convergence is very slow, and CPU utilization at the BGP Router process is always near 100 percent during the convergence at the aggregation router. This issue obviously shows the following tendencies:

1. The greater the number of component prefixes that belong to the aggregate- address entry, significantly slower convergence is seen at the aggregation router.
2. The greater the number of duplicate aggregation component prefixes for the aggregate-address entry, seriously slower convergence is seen at the aggregation router.

Conditions: Any release would be affected if “aggregate-address” is configured and routing updates are received every few seconds.

Workaround: Remove the “aggregate-address”.

Further Problem Description: If you configure “aggregate-address” lines after BGP convergence has been achieved, the BGP process only holds about 60 or 80 percent of the CPU for about 1 minute. However, if you do peer reset after “aggregate-address” entries have been configured, the convergence time is about 32 minutes (it is about 6 minutes if “aggregate-address” entries are removed).

- CSCso21463

Symptoms: A one-way voice issue is seen when making a transcoded transfer call with an H.323 endpoint.

Conditions: A one-way voice issue is observed when DSP farm resources are controlled by CCM and the transcode profile has g711alaw and g729 codecs, but no g711ulaw, configured on the DSP farm router. The checkbox for MTP required is checked under the H.323 gateway configuration page.

Workaround: Add g711ulaw in the transcode profile.

- 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.

- CSCsu25833

Symptoms: An ISR router may crash with the following error message: %ALIGN-1-FATAL: Corrupted program counter

Conditions: The symptoms are observed on a Cisco 2811 and 2801 router. The trigger has not yet been identified.

Workaround: There is no workaround.

- CSCsv73509

Symptoms: If “no aaa new-model” is configured, authentication occurs through the local even when TACACS is configured. This happens for EXEC users under the VTY configuration.

Conditions: The symptom is observed when you configure “no aaa new-model”; configure “login local” under line vty 0 4; and configure “login tacacs” under line vty 0 4.

Workaround: There is no workaround.

- CSCsv77932
Symptoms: Router crashes.
Conditions: Occurs while configuring serial interface for insufficient MTU.
Workaround: There is no workaround.
- CSCsv87146
Symptoms: Clearing of NAT translation either manually or automatically through timeout results in crash.
Conditions: Occurs when a dynamic translation mapping is removed while traffic is running.
Workaround: Stop traffic before removing dynamic NAT translation.
- CSCsw24542
Symptoms: A router may crash due to a bus error after displaying the following error messages:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error, %ALIGN-1-FATAL: Illegal access to a low address < isdn function decoded>
```

Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.
Workaround: There is no workaround.
Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.
- CSCsw52416
Symptoms: Dynamic NAT entries are not timing out properly
Conditions: Occurs even after timer expired.
Workaround: There is no workaround.
- CSCsw71188
Symptoms: A Cisco 7200 series router may lose connectivity to the SDH link.
Conditions: The symptom is observed under the following conditions:
 1. The Cisco 12416 router receives a PAIS Alarm from the Optical Network.
 2. The interfaces go down and up and the ALARM is cleared from the Cisco 12416 router side.
 3. The Cisco 7200 series router loses connectivity.
 4. The Cisco 12416 router interface POS is still UP, but the ping fails.
 5. After interface is shutdown and re-enabled, it is in serial UP but protocol DOWN from the Cisco 12416 router side.
 6. The link is recovered when the fiber is disconnected and reconnected from the Cisco 7200 series router side.
Workaround: Disconnect and re-connect the fibers from the Cisco 7200 series router side.
- CSCsx47915
Symptoms: Spurious memory access and alignment error observed when removing policy-map from interface under certain configuration sequence.
Conditions: The problem is seen on Cisco routers running Cisco IOS Release 12.4(18e).
Workaround: There is no workaround.

- CSCsx74657

Symptoms: Multiple issues are seen on multicast NAT. NAT is adding the number of dynamic entry statistics for every new multicast packet, even though there is already an existing NAT flow entry. This causes the number of dynamic entries to be inconsistent with the output from **show ip nat trans**. Also, dynamic NAT entries cannot be deleted with **clear ip nat trans ***. Finally, every fragmented multicast packet creates a separate NAT entry.

Conditions: Occurs when **ip pim sparse-dense-mode** is configured on the interfaces with NAT overload.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(18c)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(18c). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(18c). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCek74855

Symptoms: Modifying class parameters in a service policy attached to a multilink may trigger a crash, if the **show policy-map int** command is issued.

Conditions: The problem is platform independent, but it has been seen on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(13.13)T.

Workaround: There is no workaround.

- CSCse61834

Symptoms: When you modify an ATM PVC by entering the **pvc vpi/vci** command, any subsequent modifications in the VC class that is assigned to this PVC do not take effect.

Conditions: This symptom is observed when the PVC is preconfigured with a VC class when the following events occur:

- 1) You make a configuration change in the PVC.
- 2) You change the configuration in the VC class.

The configuration change in the VC class does not take effect.

Workaround: First complete the configuration changes in the VC class. Then, change the configuration in the PVC.

- CSCsl21168

Symptoms: A router crashes. Prior to the crash, the log file contains numerous messages indicating:

```
SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (2/2), process = IP NAT Ager.
```

Conditions: This symptom is observed on a router with NAT enabled.

Workaround: There is no workaround.

Further Problem Description: The fix for this defect caused a new bug: CSCso62511. Ensure that you have the fix for CSCso62511 in addition to this defect if you are encountering this problem.

- CSCsl96254

Symptoms: If an EIGRP distribute-list that is applied to an interface allows a route, the route will be installed into the routing table without first checking to see if the global distribute-list allows it as well. All platforms are affected.

```

access-list 1 permit any
access-list 2 deny any

router eigrp 1
 network 192.168.1.0 0.0.0.255
 distribute-list 1 in FastEthernet0/0
 distribute-list 2 in
 no auto-summary

```

The configuration above should deny all routes by virtue of access-list 2. Instead, all routes are allowed per access-list 1.

Conditions: Running EIGRP with interface distribute lists and a global distribute list. All platforms are affected.

Workaround: Currently the only workaround is to apply the global distribute list to each interface distribute list.

- CSCsm17767

Symptoms: On a gateway configured for ISDN Non-Facility Associated Signaling (NFAS) with a primary and backup D channel, both the primary and backup D channel interfaces may be marked “OUT OF SERVICE” if the gateway sends the first “in-service” message during a D channel switchover.

Conditions: This symptom occurs only when the gateway sends the first ISDN service message indicating that it is bringing the backup D channel in service. If the peer sends the message first, the switchover is completed successfully.

Workaround: There is no workaround.

- CSCso01307

Symptoms: On a Hot Standby Router Protocol (HSRP) standby router, all accounting records for **aaa accounting commands** and **aaa accounting system** on the standby router of the HSRP pair are available only if those two commands are applied.

Conditions: AAA accounting is configured on a router pair that is running HSRP.

Workaround: Change the router to the active state before making changes that are to be logged.

Further Problem Description: The following message will appear when the **debug aaa accounting** command is executed and a record is suppressed:

```
*<time/date>: AAA/ACCT/CMD(00000003): Suppressed record
```

- CSCso19662

Symptoms: Tracebacks are seen after unconfiguration when using the **clear ip nat translation *** command.

Conditions: This traceback occurs with the c7200-js-mz.124-18a.fc2 image.

Workaround: There is no workaround.

- CSCso53653

Symptoms: A Cisco router may leak memory if configured for an Embedded Event Manager (EEM) applet that utilizes the **action tag cli** command.

Conditions: This symptom occurs under two conditions:

- Either there is not enough memory for the action to complete properly, in which case there will be memory allocation failure messages sent to the log.
- Or there are not enough vtys available to run the action, in which case the following errors may be seen in the log:

```
%HA_EM-3-FMPD_CLI_CONNECT: Unable to establish CLI session: no more tty lines
%HA_EM-3-FMPD_ERROR: Error executing applet appletname statement tag
```

This only occurs in EEM versions 2.2 and earlier. EEM 2.2 is available in Cisco IOS Release 12.4 Mainline. EEM 2.3 and later versions are not affected.

Workaround: Increase the number of vtys so that the policy will always be able to get one. Do not run the Cisco IOS device low on memory.

- CSCso67601

Symptoms: When a call using a CMM ACT transcoder is disconnected from the H323 endpoint, the transcoder shows as being unregistered. The transcoder remains unregistered on resetting it from the CCMAAdmin page. The **show dspfarm all** command shows two active connections even though the CCM side has already cleared the call.

Conditions: The symptoms are observed when a CMM ACT transcoder is used and the call is cleared by an H323 endpoint.

Workaround: On reloading the jagger, the transcoder registers to the CCM.

- CSCso69584

Symptoms: On a CMM running Cisco IOS Release 12.4.13b with an ACT Module, several DSPs may get reset because of heartbeat errors and may cause the calls to fail. The following messages will be displayed on the console, and traceback messages may also appear:

```
Apr 3 11:59:09: ac_mtrDsp_ev(slot 0 dspId 1 heartBeat 0CDC8D38) reset[hbErr 0]
Apr 10 10:54:41: ac_mtrDsp_ev(slot 1 dspId 2 heartBeat 10718287) reset[hbErr 0]
Apr 10 10:54:41: ac_mtrDsp_ev(slot 2 dspId 1 heartBeat 107178F7) reset[hbErr 0]
Apr 10 10:54:56: ac_mtrDsp_ev(slot 2 dspId 1 heartBeat 0000058D) reset[hbErr 0]
Apr 10 10:54:56: ac_mtrDsp_ev(slot 1 dspId 2 heartBeat 000005BF) reset[hbErr 0]
Apr 10 10:55:12: %SCHED-2-EDISMSCRIT: Critical/high priority process MS_AC Dsprm Main
may not dismiss. -Process= "MS_AC Dsprm Main", ipl= 0, pid= 38
```

Conditions: This symptom is observed under normal working conditions and occurs because of unknown reasons.

Workaround: There is no workaround.

- CSCso91078

Symptoms: A Cisco IAD2430 may reload unexpectedly because of a bus error (Sig=10).

Conditions: The symptom is observed on a Cisco IAD2430.

Workaround: There is no workaround.

- CSCsq03286

Symptoms: A Cisco Communication Media Module (CMM) with an Adhoc Conferencing and Transcoding (ACT) port adaptor module configured for MTP/XCODING may get into a state where further attempts to utilize DSP resources in a transcoding profile may fail.

Conditions: Under rare conditions, a CMM module used for MTP/XCODING may see the DSP resource on the module become unresponsive. When this occurs, a DSP recovery algorithm on the CMM module will be invoked to attempt to recover the DSP resource.

This algorithm may in some circumstances leave the associated transcoding resource in a state where further calls to invoke these resources will fail.

When the DSP recovery mechanism is invoked, the following message at debug level will be logged:

```
ac_mtrDsp_ev(slot 2 dspId 1 heartBeat 0000058D) reset[hbErr 0]
```

If the recovery mechanism fails to properly recover the resources, there will be hung calls seen in the output of the **show mediacard connection** command (0 packets tx/rx will be displayed).

Further calls that attempt to use this resource will see OpenReceiveChannel failures as displayed in the output of the **show sccp statistics** command.

An example of this is below:

```
CMM-01# show mediacard connection
```

```
Id Type Slot/ RPort SPort RxPkts TxPkts Remote-Ip DSP/Ch 25 xcode 2/4/23 18300 22684 0
0 172.16.175.160 26 xcode 2/4/24 16710 22540 0 0 172.16.175.116
```

```
CMM-01# show sccp statistics
```

```
SCCP Application Service(s) Statistics:
Profile Identifier: 1, Service Type: Transcoding TCP packets rx 1676, tx 443
Unsupported pkts rx 0, Unrecognized pkts rx 0 Register tx 1, successful 1, rejected 0,
failed 0 KeepAlive tx 25, successful 25, failed 0 OpenReceiveChannel rx 412,
successful 398, failed 24 CloseReceiveChannel rx 412, successful 398, failed 14
StartMediaTransmission rx 412, successful 398, failed 14 StopMediaTransmission rx 412,
successful 380, failed 0 Reset rx 0, successful 0, failed 0 MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

Workaround: Work to prevent the DSP from becoming unresponsive.

- CSCsq12128

Symptoms: If the WAN connection is DOWN on the VGW, the Media Gateway Control Protocol (MGCP) fallback mode may not load. The gateway remains in “MGCP Fallback mode: Enabled/OFF” mode.

Conditions: This symptom is observed with Cisco IOS Release 12.4(16).

Workaround: Shut down the interface.

Further Problem Description: It is possible that the link goes up and down frequently. The call manager application tries to download the XML file from CCM+TFTP even when the link is down. This sets a flag. The flag prevents the fallback.

- CSCsq29139

Symptoms: When IPv6 prefix delegation receives periodic RENEW message from a client, it may incorrectly bind the corresponding prefix for another client.

Conditions: The symptom is observed when IPv6 prefix delegation assigns a prefix to a client that is connected via a virtual access interface.

Workaround: There is no workaround.

- CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsq60016

Symptoms: A router crashes after a long RSA key string is entered.

Conditions: This symptom is observed when a very long hex string is entered.

Workaround: Break the entry into shorter strings.

- CSCsq74300

Symptoms: Loopbacks, Null0, and other non-Point-to-Point interfaces are not allowed in a **route-map set** command because of the changes introduced with caveat CSCsk63775.

Conditions: This symptom is observed with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsq83872

Symptoms: There may be a memory leak when the **no pppoe enable** command is applied.

Conditions: This symptom is observed on a Cisco 831 router.

Workaround: There is no workaround.

- CSCsr11514

Symptoms: QoS RTP statistics are not updated correctly for a short call duration.

Conditions: Call flow:

PSTN ---(E1)---> AS5850 -(MGCP)----> Call Agent.

- Calls are less than 40 seconds.
- The **show voice active** command has not been issued (will force update).
- The RTCP timer is set to 65000.

Workaround: Reduce the **ip rtcp report interval** value on the gateway, and monitor the load.

- CSCsr16693

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPsec NAT traversal (NAT-T) feature can be used as an alternative.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml>.

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

- CSCsr20566

Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

Workaround: There is no workaround.

- CSCsr38532

Symptoms: A memory leak is observed in the CCH323_CT process when a load test is performed.

Conditions: This symptom is observed with Cisco IOS Release 12.4(18b) but not with Cisco IOS Release 12.4(19b).

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(18b)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(18b). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(18b). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCek78237

Symptoms: A short CPU hog seen in the ATM PA Helper process when an interface flaps and the framing configuration is modified on the interface.

Conditions: This symptom is observed on a Cisco 7200 with a PA-A3-T3 adapter that is running Cisco IOS Release 12.2(25)S or 12.2(31)SB (and possibly other Cisco IOS releases).

Workaround: There is no workaround.

Further Problem Description: The CPU hog is enough to cause OSPF adjacencies (with fast hello) to go down on other unrelated interfaces. The same problem is seen if BFD is configured.

- CSCsa65314

Symptoms: Inbound calls on an MGCP-controlled CAS trunk may experience symptoms where the call does not complete and the calling party hears dead air. When this occurs, it will be experienced at that particular timeslot on the digital trunk until some manual intervention is taken to correct this.

Conditions: This symptom has been observed at times on Cisco IOS VoIP gateways with CAS trunks configured from MGCP back to Cisco Unified CallManager (CUCM/CCM). An inbound call on a timeslot that is in this state will show the vtsp state in the **show voice call summary** command output as S_DIGIT_COLLECT and will not progress past this point.

Once source of this issue has been when the status of the timeslot on the CallManager and the gateway is not the same. For example, the CallManager may indicate that the channel is out of service (OOS) while the gateway has the status of this timeslot as in-service (idle). Please refer to CSCef58219, which has seen to lead to this state. If this issue is being seen because of this difference in status between the CallManager and the Cisco IOS gateway, the recommended action is to upgrade the CallManager with a release that contains the fix for CSCef58219.

Workaround: The only known workaround to prevent this issue from occurring is to use H.323 instead of MGCP with CAS trunks.

Once in this state, to recover the timeslots you can:

1. Enter the **shutdown** command and the **no shutdown** command on the voice port.
2. When there are multiple channels stuck, enter the **no mgcp** command and then the **mgcp** command.

- CSCsi03359

Symptoms: A PIM hello message may not reach the neighbor.

Conditions: This symptom is observed on a Cisco router when an interface comes up and a PIM hello message is triggered.

Workaround: Decrease the hello timer for PIM hello messages.

Further Problem Description: The symptom occurs because the PIM hello message is sent before the port can actually forward IP packets. IGP manages to get its neighborhood up but PIM does not, causing RPF to change to the new neighbor and causing blackholing to occur for up to 30 seconds.

- CSCsi83521

Symptoms: A Cisco 7200 router crashes upon execution of a sequence of permit commands under “ipv6 access-list testipv6” subconfiguration mode.

Conditions: This symptom is observed on a Cisco 7200 router that is loaded with a Cisco IOS Release 12.4(13.13)T3 image.

Workaround: There is no workaround.

- CSCsj49293

Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

Workaround: There is no workaround.

Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsl10459

Symptoms: Routers that are running Cisco IOS Release 12.4(13b) and Release 12.4(16) may crash when the **show crypto pki timers** command is executed.

Conditions: This symptom is observed under a narrow set of conditions. Offending conditions occur when certificates are issued Certificate Distribution Point formatted in URL format. Certain other unknown circumstances must also occur.

Workaround: Avoid using the **show crypto pki timers** command.

- CSCsl14450

Symptoms: Under a high load of multicast traffic, a Cisco router may unexpectedly reload due to a CPU vector 300 or bus error.

Conditions: This symptom has been observed only in environments where more than 10 tunnels have been configured on the same device using multicast over these tunnels.

Workaround: There is no workaround.

- CSCsl32142

Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with “Bad getbuffer” error may also be reported.

Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCsl67527

Symptoms: HTML pages inside a TAR file fail to load. This affects web applications such as Security Device Manager (SDM). If SDM is installed in a router’s flash, the user is unable to invoke the HTML page that is archived inside the TAR. The SDM application fails to launch, and the user will receive a “page not found” error.

Conditions: This symptom is observed only when files are contained in a TAR file. All other HTML files can be loaded successfully. For the Cisco IOS Release 12.4 train, the problem was introduced in Cisco IOS Release 12.4(17.6) and fixed in Cisco IOS Release 12.4(18.11).

Workaround: There is no workaround.

- CSCsl78850

Symptoms: When the WAN is restored between an MGCP/SRST gateway and CallManager, the MGCP gateway intermittently fails to register back with CallManager.

Conditions: Connectivity to the CallManager from the gateway is stopped. When the gateway goes in SRST, a PSTN call is placed to a phone that registers with the gateway. WAN connectivity is then restored. MGCP has one primary call agent and two redundant hosts configured.

Workaround: Reload the gateway.

Further Problem Description: When the gateway is in this “stuck” state of not registering with the CallManager, if “no ccm-manager mgcp” is configured, it does not take effect, and “no ccm-manager redundant-host ...” also does not take effect. The following error message is displayed:

```
cmapp_service_emptying_redun_hostlist: Error: cannot execute CCM host change -- must
configure again!
```

- CSCsl83415

Symptoms: After executing the following CLI commands (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

Test 10:

- a. clear ip bgp 10.0.101.46 ipv4 multicast out
- b. clear ip bgp 10.0.101.47 ipv4 multicast out

Test 1:

- c. show ip bgp ipv4 multicast nei 10.0.101.2
- d. show ip bgp ipv4 multicast [<prefix>]
- e. configure terminal

The crash does not happen for each of the following cases:

1. If the same CLI is cut-paste manually, there is no crash.
2. If the **clear cli** command is not executed, there is no crash.
3. If the **configure terminal** command is not entered, there is no crash.

Conditions: The symptom occurs after executing the above CLI.

Workaround: There is no workaround.

- CSCsm27979

Symptoms: A router crashes with “Address Error (load or instruction fetch) exception” when the **show ip vrf vrf-name** command is used.

Conditions: On one vty session, enter the **show ip route vrf vrf-name** command and leave it in the “more” condition. From other user interface session, go to configuration mode, and then enter the **no ip vrf vrf-name** command using the same VRF name. After at least 5 minutes, the router will crash after hitting the any key on the session that is doing the **show ip vrf** command.

Workaround: Make sure that there is no **show ip route vrf** command pending before entering the **no ip vrf** command.

- CSCsm55553

Symptoms: A continuous ringback tone is heard at the calling side even after the off-hook of the called side.

Conditions: This symptom is observed on an MGCP endpoint using the LCS package, after the fix for CSCsb28921.

Workaround: Use a Cisco IOS version without the fix for CSCsb28921.

- CSCsm57122

Symptoms: This is an interoperability issue of SSH and SCP among several open SSH clients and the Cisco IOS client.

Conditions: SCP is not working simultaneously with the Putty SSH client and CiscoWorks. When transferring the Cisco IOS image to the device, the CPU is being utilized heavily by the SSH process (noticed through the **show proc cpu** command). Also the file transfer rate is very low at 16 to 20 KB/s.

Workaround: There is no workaround.

- CSCsm62680

Symptoms: Dynamic NAT using a route-map with reversible fails to allow outside-inside traffic when the route-map has a deny statement first.

Conditions: This symptom is observed when the route-map is configured.

Workaround: Remove the route-map deny statement, or use an ACL.

- CSCsm92206

Symptoms: A router may crash when a range of interfaces is set to default configurations.

Conditions: The crash occurs when a range of interfaces is configured in a console connection to belong to a bridge group and when the same set of configurations is removed simultaneously from a vty connection.

Workaround: Avoid simultaneous tasks (configuring/unconfiguring) through the console and vty.

- CSCsm96833

Symptoms: A router may crash when a multicast packet is forwarded on a tunnel interface.

Conditions: This symptom is observed when multicast routing and egress NetFlow are enabled. This is a platform-independent bug.

Workaround: Disable egress NetFlow on the tunnel interface.

- CSCso15151

Symptoms: When Multicast Distributed Fast Switching is configured, a VIP crashes on a Cisco 7500 router that is running a Cisco IOS 12.3 release.

Conditions:

1. The router has around 1000 interfaces/subinterfaces.
2. Distributed multicast is configured.
3. The router is running any Cisco IOS 12.3 release.

Workaround: There is no workaround.

Further Problem Description: In summary, the line card is accessing the memory location that has been freed already. This results in the VIP crashing. There are sanity checks that are missing in Cisco IOS 12.3 releases. The problem is similar to what bug CSCdm29808 does on line cards of the Cisco 12000 Internet series router (this router does not support Cisco IOS Release 12.3). This basically checks if the interface index on MDFS messages is less than the MDFS Idb map size, which indicates the current size of the Idb map table.

- CSCso38649

Symptoms: Memory leaks are seen on a SIP-TDM gateway, leading to low available memory. Low memory can cause no access to the console and can also negatively affect normal functionality.

Conditions: This symptom is observed when supplementary services are invoked on a SIP-TDM gateway that is running Cisco IOS Release 12.4(13e).

Workaround: There is no workaround other than reloading the router.

- CSCso54391

Symptoms: An MLPP call receiving preemption for reuse on unanswered call from the PBX fails to complete.

Conditions: This symptom is observed on all platforms.

Workaround: There is no workaround.

- CSCso78427

Symptoms: A voice gateway is crashing at ccsip_apply_sip_to_pstn_calling_policy with a TLB (store) exception.

Conditions: This symptom is observed on a Cisco AS5400XM that is running either Cisco IOS Release 12.4(19) or Cisco IOS Release 12.3(14)T6.

Workaround: There is no workaround.

- CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.

This security advisory is being published simultaneously with announcements from other affected organizations.

- CSCsq13348

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>.

Resolved Caveats—Cisco IOS Release 12.4(18a)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(18a). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(18a). This section describes severity 1 and 2 caveats and select severity 3 caveats.

- CSCek76062

Symptoms: A router crashes because of a block overrun (overwriting the memory block).

Conditions: This symptom is observed only when templates are exported in the export pak, which is used only in version 9 version of exporting.

Workaround: Version 5 could be used for exporting.

- CSCsg16778

Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

Workaround: There is no workaround.

Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- CSCsh22725

Symptoms: Outbound calls fail on a MGCP-controlled CAS channel on a Cisco VoIP gateway.

Conditions: This symptom is observed when the following conditions occur:

- A timeslot on an E&M T1 trunk is taken out of service from the connected switch side, showing as a permanent inbound seizure. In this situation, the output of the **show voice call summary** command indicates that the status for this channel is “EM_PARK”.
- A Cisco CallManager that interworks with the Cisco VoIP gateway checks the status of the trunk via an MGCP AUEP command. The gateway responds with an “ES: rlc” message, which indicates that the trunk is available for calls.

Because the reported availability and actual availability of the channel are mismatched, all outbound calls on the channel fail.

Workaround: Attempt to clear the out-of-service state from the connected switch side. If this is not possible, when interworking with the Cisco CallManager, first enter the **shutdown** command followed by the **no shutdown** command on the voice port and then enter the same commands on the T1 controller. Doing so causes the gateway to send an NTFY message that indicates that there is an inbound seizure on the channel.

- CSCsi20225

Symptoms: Continuous tracebacks may be generated on an LNS.

Conditions: This symptom is observed when you bring up PPPoX or L2TP sessions over multiple tunnels without traffic being processed over these sessions.

Workaround: There is no workaround.

- CSCsi73481

Symptoms: PPPoE sessions may fail to establish on IDBless/ambiguous VLAN.

Conditions: PPPoE sessions served on a VLAN not associated with an ethernet subinterface may fail to come up because PPP packets are being sent without an 802.1Q header. This only happens when there is no subinterface configured with the native 802.1Q VLAN.

Workaround: A workaround is to configure a subinterface with the native VLAN.

- CSCsj46178

Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router in either global MGCP configuration or MGCP profile.

Workaround: Do not configure the **endpoint naming t3** command. Use t1 endpoint naming instead.

- CSCsj49255

Symptoms: If there is an ACL and DSCP being used for packet matching on class- map, only the first packet descriptor will get a match, and everything else will not. If DSCP is removed, the packet matching works again.

Conditions: This symptom is observed on a Cisco 7200 with ACL and DSCP with match all option.

Workaround: There is no workaround.

- CSCsj74812

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: Occurs when running show commands on an exec session that has been established through one of the integrated modems on a WIC-AM or WIC-2AM. This would only be seen on async cards with gt96k, hwic or pquicc drivers.

Workaround: There is no workaround.

- CSCsj89544

Symptoms: If a BGP keepalive message fails to be sent to a BGP peer because the transport link is down, the neighbor BGP peer does not accept any further keepalive packets even though TCP retransmits the failed message using a backup path. This eventually causes the BGP peer to go down because of holdtime expiration.

Conditions: This happens when TCP retransmissions occur on MPLS-enabled network. This is seen only when MPLS is configured on Catalyst 6500 or Cisco 7600.

Workaround: There is no workaround.

- CSCsj93012

Symptoms: A Cisco 7500 router may crash when QoS is enabled.

Conditions: Occurs when ATM and serial interfaces have QoS configurations as output/input policy and when peer is reloaded.

Workaround: There is no workaround.

- CSCsk25651

Symptoms: With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM)/CallManager and utilizing SRST functionality, when the IP phones are registered to the SRST router, the message-waiting indication (MWI) states may be incorrect.

Conditions: When a phone registers to a Cisco SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come, first-served fashion. The MWI state, however, is remembered from the previous registration that used that ephone-dn number so the MWI status could be incorrect.

Workaround: Configure both the SRST router and the CUE to use SUBSCRIBE/NOTIFY MWI method.

- CSCsk26774

Symptoms: Native VLAN information is not included in CDP packets going out ports of an EtherSwitch (ESW) module in Cisco 28xx and Cisco 38xx routers. All the platforms using switchports (of any kind built-in/NM/WIC/HWIC) have this issue: Cisco 8xx, Cisco 17xx, Cisco 18xx, Cisco 26xx, Cisco 36xx, Cisco 37xx, Cisco 28xx, and Cisco 38xx.

Conditions: This symptom causes Cisco IP phone models 7961, 7941 and 7970 that are running SCCP firmware to fail to forward traffic coming from a PC connected at the back of the phone.

Workaround: Enable the “Voice VLAN Access” setting on the phone.

- CSCsk27147

Symptoms: The following SNMP is incorrectly generated:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
This issue is affecting the CISCO-MEMORYPOOL-MIB instead.
```

Conditions: Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

Workaround: Exclude ciscoMemoryPoolMIB from your query with the following commands:
snmp-server view public-view iso included snmp-server view public-view ciscoMemoryPoolMIB excluded Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

- CSCsk35970

Symptoms: Excessive CPU usage occurs on a Cisco 12000 Series Router running Cisco IOS Release 12.0(32)S and configured for BGP multipath with several iBGP and eBGP peers.

Conditions: TblVer is incrementing every 5 minutes, causing the BGP router process to use maximum CPU every 5 minutes.

Workaround: There is no workaround.

- CSCsk40676

Symptoms: The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Conditions: Occurs when LZS compression is used on a Windows Vista client.

Workaround: Disable LZS compression.

- CSCsk65601

Symptoms: PPP tunnel does not come up after PE edge interface flapped.

Conditions: This symptom is observed on a Cisco router when the **show mpls l2transport vc** command is entered.

Workaround: Use the **xconnect** command to unconfigure and then reconfigure the xconnect under the serial interface being flapped to restore.

- CSCsk78725

Symptoms: While giving T1 controller configuration, the router crashes. This happens on the 8-port multichannel T1/E1 8PRI PA (PA-MC-8TE1+).

Conditions: Occurs on a router running Cisco IOS Release 12.4(17.7) and Cisco IOS Release 12.4(17.4)T1.

Workaround: There is no workaround.

- CSCsk88637

Symptom:

OAM cells are not generated when a new ATM subinterface and PVC is configured. Subinterface status is up/up, PVC is down. No debug output is seen with **debug atm oam interface atm/x.xxx** command.

Conditions: Occurs when new ATM subinterface and PVC is configured.

Workaround: Perform **shut/no shut** commands on ATM subinterface.

- CSCsk94179

Symptom: Connectivity problems are observed for IPv6 client, which obtained IPv6 prefix via DHCP for Virtual Access interface, due to incorrect static routes in the routing table for the assigned IPv6 prefix.

Conditions: Occurs with IPv6 prefix delegation via DHCP, when client moves from one interface to another.

Workaround: None

Further problem description: When IPv6 prefix delegation assigns a prefix for Virtual Access interface, it creates a static route for the prefix in the routing table. When a client moves to a new interface, old binding and the old routes are retained, which causes the problem.

- CSCsk97130

Symptoms: VXML application causes memory leak

Conditions: If the calling document and called document of a subdialog share the same root document, the tree structure used for the root document will not be released after the call session is finished.

Workaround: There is no workaround.

- CSCsk97384

Symptoms: Abnormally large FreshTime value appears in IVR HTTP client cache entry.

Conditions: This symptom is observed when a VXML voice browser downloads a file from an HTTP server. If the file was modified very recently, the FreshTime for that file may show up with a very large value.

Workaround: There is no workaround.

- CSCsl04516

Symptoms: A Cisco router may experience the following errors:

```
Jan 11 07:06:58: %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x476292F0 -Process= "Skinny
Socket Server", ipl= 0, pid= 260 -Traceback= 0x41259724 0x41A50418 0x41A54754
0x41A28134 0x41A2AFA4 0x41A2F30C 0x4095AB80 0x4095B5F4 0x423CD6E4 0x423CD6C8 Jan 11
07:06:58: %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x476292F0 -Process= "Skinny Socket
Server", ipl= 0, pid= 260 -Traceback= 0x41259724 0x41A50418 0x41A54754 0x41A28134
0x41A2AF24 0x41A2F30C 0x4095ABA4 0x4095B5F4 0x423CD6E4 0x423CD6C8
```

Phones running over secure channels will have registration problems.

Conditions: Occurs on a Cisco 2821 router running Cisco IOS Release 12.4(18).

Workaround: There is no workaround.

- CSCsl08480

Symptom:

The following error messages are seen Memory allocation failed atm_vpivci_to_vc with subsequent device crash.

Conditions: Observed with incoming ATM traffic.

Workaround: None.

- CSCsl14635

Symptoms: T38 negotiation is failing for an incoming UPDATE request that has a T38 offer.

Conditions: This symptom occurs when the voice gateway is running Cisco IOS Release 12.4(15)T and is processing incoming Session Initiation Protocol (SIP) calls. When the SIP call is active and an UPDATE request is received that contains a T38 offer, the UPDAE request is rejected. The switchover from voice to fax fails.

Workaround: Fax over T38 works fine when midcall INVITE is used for T38 negotiation.

- CSCsl17539

Symptoms: A Cisco router may reload with the following symptoms:

```
Oct 31 22:55:21.282: %SYS-3-MGDTIMER: NZ prev pointer but not running, timer =
64C37818. - Process= "IP Input", ipl= 4, pid= 66 -Traceback= 0x60746048 0x6084EA34
0x6084F14C 0x62333AD8 0x62337C70 0x62306494 0x623068B0 0x60A40654 0x60A416F8
0x60A41778 0x60A41964 Oct 31 22:55:48.894: %SYS-3-MGDTIMER: Setting zero expiration
time, timer = 64132350. -Process= "IPSEC key engine", ipl= 4, pid= 150 -Traceback=
0x60746048 0x6084E9A8 0x6084FA18
22:55:48 zulu Wed Oct 31 2007: Address Error (load or instruction fetch) exception,
CPU signal 10, PC = 0x60815B08
0x60815B08 0x6084FCA4 0x622B2E54 0x622B39C4
```

Conditions: Occurred on a Cisco 7206VXR running Cisco IOS Release 12.4(16).

Workaround: There is no workaround.

- CSCsl21123

Symptoms: Entering the **dir stby-harddisk:** command causes the active RP to crash.

Conditions: Occurs on a Cisco 7600 router.

Workaround: There is no workaround.

- CSCsl24858

Symptoms: Cisco 7200 router with PA-VXC/B may go into “hang” state and fail to respond to console.

Conditions: Occurs on a Cisco 7200 router with PA-VXC/B and configured for active calls over the PA.

Workaround: There is no workaround.

- CSCsl32408

Symptoms: SIP gateway does not pass privacy information to the ISDN leg.

Conditions: The voice gateway is running Cisco IOS Release 12.4(15)T and processing incoming session initiation protocol (SIP) calls. When a SIP message is received on the voice gateway with calling number containing non-digit (calling number preceded by a '+'), then octet_3a information present in the SIP message is not passed to the ISDN leg.

Workaround: There is no workaround.

- CSCsl34303

Symptoms: Cisco 7200 router crashes when unconfiguring service policy from Multilink Frame Relay (MFR) interface.

Conditions: Occurs if one of the MFR bundle link interfaces was previously being used for Multilink PPP over Frame-relay. Changing the encapsulation may not clean up queuing configuration properly - a dual first in first out (FIFO) queue may remain on the interface.

Workaround: Ensure a dual FIFO queue is not present on MFR bundle link interface. It should be plain FIFO queue. If it is a dual FIFO, change the interface to HDLC encapsulation, which should remove the dual FIFO queue, then back to MFR bundle link encapsulation.

- CSCsl43394

Symptoms: Standby RSP reloads and has problems syncing configuration when DS1 controller is removed from DS3 configuration.

Conditions: This problem is seen when SSH is enabled on the router and DS1 controller is added or deleted from the configuration.

Workaround: There is no workaround.

- CSCsl54748

Symptoms: DHCPv6 bindings for multiple clients are stored in a virtual-access interface when each different user has the same DHCP Unique Identifier (DUID).

Condition: This problem is observed when a router is configured for PPPoE or L2TP LNS and is working as DHCPv6 prefix delegation (PD).

Workaround: There is no workaround.

- CSCsl61416

Symptoms: Certain prompts will not play properly. Dead air is heard and call disconnects.

Conditions: Occurs on a Cisco AS5350 acting as a VXML gateway in an IPCC environment and running Cisco IOS Release 12.4(7)b using streaming prompts.

Workaround: Turn off streaming mode. Reloading the gateway temporarily fixes the issue.

- CSCsl62609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsl63494

Symptoms: When user dials into Cisco AS5350 and initiates X.25 session, then disconnects the line, the session is not freed up. The next time the user dials in, a "max session reached" error occurs.

Conditions: Occurs with Cisco AS5350 and CiscoSecure ACS as TACACS server.

Workaround: There is no workaround.

- CSCsl70143

Symptoms: Under heavy traffic, ISDN calls may be rejected due to high CPU usage with the following messages seen in the log (with tracebacks):

```
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (98/100). Call (callID=23524) is rejected.
```


%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (32/18),process = ISDN.

Conditions: This problem occurs only under heavy traffic.

Workaround: There is no workaround.

- CSCsl70722

Symptoms: A router running Cisco IOS may crash due to watchdog timeout.

Conditions: Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon MIB for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

Workaround: There is no workaround.

- CSCsl87400

Symptoms: H323 setup message is malformed after NAT translation

Conditions: Setup message includes the neededFeatures, desiredFeatures, supportedFeatures extensions.

Workaround: Do not use the extensions listed above.

- CSCsl90187

Symptoms: Low memory leak may occur on VoIP gateway in VTSP process, which may cause router to reload.

Conditions: The issue is specific to the C549 DSPs on Cisco 3700 series routers. The leak occurs when a call is disconnected due to non-availability of the circuit (cause code 0x22).

Workaround: There is no workaround.

- CSCsl92595

Symptoms: After 3 minutes of normal operation, packet loss occurs over Dialer PPP multilink (MLPPP enabled) interfaces.

Conditions: Occurs when CEF is enabled and “ip address negotiated” is configured on the interface.

Workaround: Use one of the following options: Permanent: disable CEF with the **no ip cef** command. Permanent: configure a static IP address on the interface. Temporary: Use the **clear adj** command to refresh all adjacencies (will last 3 minutes).

- CSCsl94410

Symptoms: CPU hog condition occurs because of stressful BGP configuration.

Conditions: Occurs in Cisco IOS releases in which CSCsl94410 has been fixed.

Workaround: There is no workaround.

- CSCsl95431

Symptoms: A router may reload when malformed packets are sent to the TFTP UDP port.

Conditions: This symptom is observed when malformed traffic is sent to the router’s TFTP UDP port 69.

Workaround: There is no workaround.

- CSCsm08291

Symptoms: Virtual access interfaces flap, and the following error message is displayed:

%SYS-2-BADSHARE: Bad refcount in datagram_done.

Conditions: Occurs on a Cisco 7206VXR with NPE-G2 and running Cisco IOS Release 12.4.(11)T1.

Workaround: There is no workaround.

- CSCsm12247

Symptoms: A Cisco IOS router configured for WCCP may stop redirecting traffic following a change in topology.

Conditions: The router must be configured for WCCP redirection using the hash assignment method. When there is only a single appliance in the service group, the loss of hash assignment details is permanent. However with multiple appliances in the group, the loss of assignment information is transitory; the router soon recovers.

Workaround: To recover the assignment details, the WCCP configuration needs to be removed and re-added to the router. Use the **no ip wccp service** command followed by **ip wccp service args** command.

- CSCsm17110

Symptoms: When setting the “FlipAddr” attribute in an IPS signature, one expects the attacker and victim TCP/IP addresses to be swapped. This is not occurring as expected and signature actions will be created against the improper TCP/IP address.

Conditions: Edit an IPS signature and set the “FlipAddr” attribute to True. Receive traffic that should cause the edited signature to fire. If a deny action is configured, the destination/victim TCP/IP address will be used instead of the expected source/attacker TCP/IP address.

Workaround: There is no workaround.

- CSCsm17414

Symptoms: When prompts are being played, the barge-in type-ahead feature works intermittently. During the menu playout, user will make a selection that should stop the rest of the menu from being played. The user is not able to stop the menu playout despite making a selection. Once the menu finishes the prompt accepts the correct digit.

Conditions: Occurred in the Cisco Customer Voice Portal (CVP) VXML application running on Cisco IOS Release 12.4(15)T1. CVP version was 3.1 SR2. CVP VXML Server and Studio 3.1. ICM 7.0 SR4 ES42.

Workaround: Combine two prompts into one.

- CSCsm17879

Symptoms: After putting the onboard GE0/0-1 interfaces into promiscuous mode, they still will not accept packets with destination MAC other than the broadcast and the interface MAC.

Conditions: This affects the onboard GE interfaces only.

Workaround: Use FE/GE ports from a module to achieve this, if available.

- CSCsm20351

Symptoms: AAL2 trunk alarm is not generated for a resource availability indication (RAI) condition when a T1 is disconnected from a VWIC module.

Conditions: This issue is seen when AAL2 trunking is configured on a Cisco 2811 running Cisco IOS Release 12.4(17a)

Workaround: There is no workaround.

Further Problem Description: This issue is not seen on non-ISR platforms running Cisco IOS Release 12.3.

- CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>

- CSCsm27726

Symptoms: After overwriting DHCP pool and client pool, status of client is IDLE.

Conditions: Occurs on Cisco routers running a pre-release version of Cisco IOS Release 12.4(17b).

Workaround: There is no workaround.

- CSCsm27943

Symptoms: When **dls w timer explorer-wait-time** is set, Ethernet redundancy could not establish DLSW circuit sometimes with the following message in the debug:

```
Jan 15 15:32:22.643 JST: DLSW-ER:(CSM):startdl_pend timer expired for transparent circuit
```

Conditions: The symptom only occurs when the router is configured for **dls w timer explorer-wait-time** with DLSw Ethernet Redundancy and **dls w transparent switch- support**.

Workaround: There is no workaround.

- CSCsm34632

Symptoms: PPTP connection does not get established properly. Users are stuck in authentication phase

Conditions: Occurs when PPTP server is behind a NAT router configured with a static NAT entry.

Workaround: There is no workaround.

- CSCsm37058

Symptoms: A Cisco 3845 router repeatedly reloads upon boot up.

Conditions: Occurs after the router is upgraded from Cisco IOS Release 12.4(5b) to Cisco IOS Release 12.4(18).

Workaround: There is no workaround.

- CSCsm45113

Symptoms: Router may install duplicate routes or incorrect route netmask into route table. It could happen on any routing protocol. The problem is introduced by CSCsj50773. See the Integrated-in field of CSCsj50773 for affected images.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The **clear ip route *** command can restore the route table until next polling of ipRouteTable MIB.

Workaround: Do not poll ipRouteTable MIB. Instead poll newer replacement MIB, ipForward MIB. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

- CSCsm48415

Symptoms: Cisco Customer Voice Portal (CVP) does not release the port if a user hangs up during database look up.

Conditions: Occurs with the following software configurations: - CVP 3.0 and Cisco IOS Release 12.4.(3g) - CVP 4.1 and Cisco IOS Release 12.4(15)T

Workaround: There is no workaround.

- CSCsm50498

Symptoms: During normal operation of Gateway Load Balancing Protocol (GLBP), when state changes from active to listen, the router stops forwarding traffic destined to the virtual MAC. Router still responds to the interface MAC.

Conditions: Occurs on Cisco 1700 routers running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCsm88305

Symptoms: A router running Cisco IOS may crash with a bus error.

Conditions: This is seen on the Cisco 2800 series platform when one or both of the onboard ethernet ports are configured as part of an etherchannel. Under low to medium traffic loads, the device may crash when executing **show run** or **write mem** commands. It also might crash without user intervention under high traffic loads.

Workaround: Do not use the etherchannel feature for onboard ethernet ports on the Cisco 2821.

- CSCsm89475

Symptoms: No output is seen from the **show policy-map interface** command when **service-policy output OUT_WAN** is configured on ATM interfaces when router is receiving QoS traffic from testing device.

Conditions: Observed on a Cisco 3800 series router. May affect other mid-range routers.

Workaround: There is no workaround.

- CSCsm89642

Symptoms: Cisco router may experience bus crash when the **show crypto sessions** command is entered.

Conditions: Occurred on a Cisco 7301 router configured as an VRF-aware IPSEC EzVPN server with clients using RADIUS x-authentication.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(18)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(18). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(18). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCsj16007

Symptoms: A PDSN member reloads at find_elt.

Conditions: This symptom is observed on a PDSN using Cisco IOS Release 12.3 (14)YX8.

Workaround: There is no workaround.

- CSCsk14633

This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007, regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

<http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html>

The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

<http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html>

Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only), and entitled “PRP crash by show ip bgp regexp,” which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

The full text of this response is available at:

<http://www.cisco.com/warp/public/707/cisco-sr-20070912-regexp.shtml>

- CSCsk70446

Cisco IOS emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

A traceback appears after the error message. This traceback is encountered with long URLs.

It is important to note that this error message does not imply that packet data is corrupted. However, it does provide an early indicator of other conditions that can eventually lead to poor system performance or a Cisco IOS restart.

- CSCsl13216

Symptoms: A warm upgrade causes a TLB exception.

Conditions: This symptom is observed with a warm upgrade to a large image using a small image such as a kboot image.

Workaround: Use normal upgrade method; that is, use “reload” command (instead of “reload warm file <image-path>”) to return to rommon and then boot the new image.

- CSCsl18054

Symptoms: A local user created with the one-time keyword is removed with unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, but under some conditions, it is removed even with failed logins.

Conditions: This symptom is observed on a Cisco IOS router.

Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsk39642

Symptoms: A router crashes.

Conditions: This symptom is observed when you are running Cisco IOS Release 12.4(17) or Release 12.4T and when you copy the saved configuration to the running configuration.

Workaround: There is no workaround.

IBM Connectivity

- CSCsj28498

Symptoms: A router may eventually experience depletion in the small buffer pool, leading to MALLOCs and Cisco IOS software crashing.

Conditions: This symptom is observed on a router running STUN SDLC with local-ack and having multiple SDLC primary stations connected and regularly polling (SNRM) router while the remote STUN peers are disconnected (no IP connectivity to the remote STUN peers).

Workaround: There is no workaround.

Interfaces and Bridging

- CSCsj71998

Symptoms: An ATM interface loses its assigned IP address if the interface is gracefully stopped/started.

Conditions: This symptom is observed in Cisco IOS Release 12.4(17).

Workaround: Reconfigure the interface.

IP Routing Protocols

- CSCsa73179

Symptoms: Memory corruption, possibly leading to a crash or other undesired behavior, can occur when the **no default-information originate** command is entered in router RIP configuration mode.

Conditions: This symptom occurs only if both the RIP routing protocol and the OSPF routing protocol are configured on a router.

Workaround: There is no workaround.

- CSCsi76616

Symptoms: LDAP packet is modified while passing through NAT router, causing LDAP to fail.

Conditions:

Network Topology

LDAP server----->(fa00)NAT Router(fa01)----->LDAP client

The packet after the NAT router seems to have been fragmented and expanded to two parts in LDAP:

Case1: LDAP failed without “no-payload”

- case1_before_nat_router -----> NAT Router -----> case1_after_nat_router
- LDAP packet modified

Case2: LDAP passed with “no-payload”

- -case2_before_nat_router -----> NAT Router -----> case2_after_nat_router
- LDAP packet unchanged

Workaround: There is no workaround.

- CSCsj00161

Symptoms: OSPFv3 may install into the routing table IPv6 routes load balancing between paths to Null0 and reachability path over the physical interface.

Conditions: This symptom may be seen if the **summary-address** command is configured with exactly the same address as one of the external routes received from a different router.

Workaround: There is no workaround.

- CSCsj39538

Symptoms: Router tracebacks and then crashes during deconfiguration (removal) of VRF. The following message was seen prior to crash:

```
-Process= "IP RIB Update", ipl= 3, pid= 68 -Traceback= 609538D8 60D1B8B4 612B2838
612588C8 61258CD4 6125E61C 6125ED04 6125EF30 61261CDC 6125A14C 61265A08 6126BE10
6097CF00 609547D8 609548B8
```

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x609538FC
```

Conditions: No specific conditions are known to cause this fault.

Workaround: There is no workaround.

- CSCsk16904

Symptoms: A NAT router fails a H323 connection by ARP resolution failure, which ARP request is triggered by H225/H245 packet. When the problem occurs, the NAT router creates an incomplete entry and sends an unexpected ARP request for the destination IP address instead of the next-hop IP address, whereas the destination prefix is not a directly connected route. Therefore if the next-hop router of NAT router disables proxy ARP, the packet forwarding fails. Ping to same destination succeeds when the problem occurs.

Conditions: This problem happens under the following conditions:

- Static NAT or dynamic NAT is configured.
- The next-hop router of NAT router disables proxy ARP.
- H323 terminal device tries to call for another one over NAT router.

Workaround: Enable proxy ARP on the next-hop router.

- CSCsk35985

Symptoms: The system crashes when the **show ipv6 ospf lsdb-radix** hidden command is entered.

Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

- CSCsk36324

Symptoms: On a Cisco router, OSPF might go into a loop during SPF calculation, causing high CPU utilization and rendering the router inaccessible.

Conditions: This symptom occurs when router LSAs with a link metric disallowed by RFC 2328 are present in the network (note that Cisco routers do not originate such LSAs) and when the network is unstable (link flapping during the SPF calculation).

Workaround: To fix the problem, reload the router. To prevent the problem, manually configure a link metric according to RFC 2328.

Important Note: CSCsk36324 caused MPLS TE defect CSCsl18176 and has been backed out under defect CSCsl18176. A new fix for this issue will be committed under defect CSCsl32318.

- CSCsk39804

Symptoms: The multicast Connection Admission Control (CAC) state may be incorrect after multicast routes have been cleared.

Conditions: This symptom is observed on a Cisco router that has Source Specific Multicast (SSM)-mapped channels that are locally joined on the router.

Workaround: There is no workaround.

- CSCsk49705

Symptoms: The **ip nat inside source static network** command does not have the <cr> option.

Conditions: This symptom is observed on a Cisco 7200 router that is loaded with Cisco IOS Release 12.4 or 12.4T.

Workaround: There is no workaround.

ISO CLNS

- CSCsj72039

Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

Workaround: Remove and reconfigure the **passive-interface** command.

First Alternate Workaround: Enter the **clear isis *** command.

Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

Miscellaneous

- CSCek67305

Symptoms: The vaccess for an APN has no IP address.

Conditions: This is very rare symptom that occurs under the following conditions:

- An APN is configured with a DHCP server that is assigning IP addresses.
- A high number of PDP are deleted followed by these PDP being created within 5 seconds.
- The above is repeated, and the vaccess for this APN loses its IP address.

Workaround: There is no workaround.

- CSCek71877

Symptoms: IPv6 pings are not working when the **atm route-bridged ipv6** command is configured on the UUT.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(13.5)T images.

Workaround: There is no workaround.

- CSCek75633

Symptoms: A router may crash when you attach a VC class to an ATM bundle.

Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

Workaround: There is no workaround.

- CSCek78330

Symptoms: A router that is configured with ATM PVCs may generate the following type of error messages:

```
%COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual- Access2.1
linked to wrong idb Virtual-Access2.1
```

Conditions: This symptom is observed on a Cisco router that has virtual-template subinterfaces.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **no virtual-template subinterface** command, save the configuration to the startup configuration, and reload the router.

- CSCsa83881

Symptoms: An interface of a PA-T3+ port adapter remains up during an Unavailable Seconds (UAS) condition that occurs because of a high C-bit or P-bit error rate.

Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-T3+ port adapter.

Workaround: There is no workaround.

- CSCsb84050

Symptoms: Cisco IOS authentication proxy does not work when both HTTP and HTTPS servers are enabled.

Conditions: This symptom is observed when HTTPS is enabled in parallel with HTTP.

Workaround: Disable HTTPS.

- CSCse85151

Symptoms: Cisco Catalyst 4500 Supervisors and Cisco Catalyst 4948 that are running Cisco IOS Release 12.2(31)SG crash when one of the following commands are issued:

- **show buffers all**
- **show buffers assigned**
- **show buffers input-interface**

Conditions: This symptom occurs when one of the following commands is issued:

- **show buffers all**
- **show buffers assigned**
- **show buffers input-interface**

Workaround: Do not use any of the above commands. For troubleshooting high CPU issues, use the steps indicated in the following tech tip instead:

http://www.cisco.com/warp/public/473/cat4500_high_cpu.html

- CSCsf11944

Symptoms: A router crashes due to the stack for process Exec running low when configuring the **auto qos** command on an ATM subinterface.

Conditions: The symptom has been observed on a Cisco router loaded with Cisco IOS interim Release 12.4(10.5).

Workaround: There is no workaround.

- CSCsg49810

Symptoms: Power fluctuation causes the Cisco VG224 to go into ROMMON mode.

Conditions: This symptom occurs while the Cisco VG224 is booting up. If the power is switched off after the initial boot message and then switched back on, the router goes into ROMMON mode.

The power off/on simulates possible power flaps.

Workaround: There is no workaround. Avoid cycling the power during bootup.

- CSCsg65318

Symptoms: Malformed SSH version 2 packets may cause a memory leak.

Conditions: This symptom is observed on a Cisco platform configured for SSH version 2 after it has received malformed SSHv2 packets. The impact of this flaw is that the affected platform may operate in a degraded condition. Under rare circumstances, it may reload to recover itself.

Workarounds: Options consist of using SSH version 1 in the interim until the affected platform can be upgraded to a fixed release or permitting only known trusted hosts/networks that can connect to the router by using a VTY access list.

Following are examples of the workarounds:

Configure SSH Version 1

```
!-- Configure from global config mode.
!
configure terminal
!
ip ssh version 1
end
```

Configure VTY Access List

```
!-- 10.1.1.0/24 is a trusted network that
!-- is permitted access to the router; all
!-- other access is denied.
!
access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any
!
line vty 0 4
access-class 99 in
end
```

More information about configuring VTY access lists is available in the *Cisco IOS Security Configuration Guide* (Release 12.4T):

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4t/sec_secure_connectivity_12_4t_book.html

More information about SSH on IOS is available in the *Configuring Secure Shell on Routers and Switches Running Cisco IOS* guide:

<http://www.cisco.com/warp/public/707/ssh.shtml>

- CSCsg91306

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsh13668

Symptoms: The following error message is generated, the console port is not longer accessible and the device stops forwarding traffic.

```
%SYS-2-NOTQ: unqueue didnt find 0 in queue 6481FC50 -Process= "<interrupt level>",  
ipl= 1
```

Conditions: The symptom is observed on Cisco routers running Cisco IOS Release 12.4 when a fiber is plugged into a PA-A3-OC3. CEF is not enabled on the ATM interface and a service-policy is applied to the ATM-interface.

Workaround: There is no workaround.

- CSCsh91974

Symptoms: The Route Processor (RP) crashes.

Conditions: Some of the Protocol Independent Multicast (PIM) CLI commands are causing the active RP to crash. The crash happens *only* when these commands are configured while in control-plane policing subconfiguration mode. Normally, any global relevant configuration should automatically exit the subconfiguration prompt and also accept the command. In this case, the PIM command is rejected and the RP crashes. The same PIM commands work fine when entered under global configuration mode (where they belong) or under other subconfiguration modes.

Workaround: Use the **exit** command to exit the main configuration prompt before configuring PIM-related commands.

- CSCsi09549

Symptoms: CPU HOG messages are displayed, and phones are deregistered.

Conditions: This symptom is observed very rarely when MoH is configured to be played from flash. Specifically, this symptom is observed under either of the following two conditions:

1. When polling ciscoFlashMIB.
2. When playing MoH for more than 30 minutes and also *once* during a h/w conference.

Workaround: The system will recover by itself after some time. Formatting flash: will also solve the issue temporarily.

- CSCsi57927

Symptoms: A Cisco router running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 will show TCP connections hung in CLOSEWAIT state. These connections will not time out, and if enough accumulate, the router will become unresponsive and need to be reloaded.

Conditions: This symptom occurs on a Cisco router running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 when executing a **copy source-url ftp:** command and the FTP server fails to initiate the FTP layer (no banner) but does setup a TCP connection. This may occur when the FTP server is misconfigured or overloaded.

The CLI command will timeout, but will not close the TCP connection or clean up associated resources. The FTP server will eventually answer and timeout itself, and close the TCP connection, but the router will not clean up the TCP resources at this time either.

Workaround: Manually clear TCP resources using the **clear tcp** CLI command, referencing the **show tcp brief** command output.

- CSCsi77147

Symptoms: DTMF path confirmation is not received for a SIP call.

Conditions: This problem is due to an issue with the SIP state machine, which may result in an error along the lines of the following:

```
00:05:10: //-1/xxxxxxxxxxxx/SIP/Error/sipSPISipIncomingMsg: Invalid method for
(STATE_IDLE): ACK
```

The call state should not be IDLE.

Workaround: There is no workaround.

- CSCsi80057

Symptoms: “Conditional default origination” into RIPv2 does not work correctly in some situations.

1. When the watching network is not present, the default route is not deleted from the local RIP database. This leads the router to still send the default route.
2. When the watching network is present, the default route is not added to the local RIP database. This leads the router to not send the default route.

Conditions: This symptom is observed if the **default-information originate route-map map-name** router RIP configuration command is used in order to generate a default route only when the watched network is present.

Workaround: There is no workaround.

- CSCsi81891

Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

Workaround: There is no workaround.

- CSCsi98120

Symptoms: A router may crash because of a bus error. Spurious accesses may be observed.

Conditions: This symptom is observed on a Cisco 7200 series router that has an NPE-G1 and that runs Cisco IOS Release 12.3(22). The router is configured as a PE router and uses MQC hierarchical policies for some subinterfaces and the legacy **rate-limit** command for other subinterfaces.

Workaround: There is no workaround.

- CSCsj07189

Symptoms: Entering the **snmpget** of an object identifier (OID) using the interface index (ifIndex) value of an interface for its index will result in an error:

```
snmpget -c <community> -v1 <device> IF-MIB::ifDescr.92
```

```
Error in packet Reason: (noSuchName)
There is no such variable name in this MIB.
Failed object: IF-MIB::ifDescr.92
```

Conditions: This can occur after port adapters (PA) have been swapped, such as replacing a 4-port PA with an 8-port PA.

Workaround: Use the **snmpwalk** to retrieve the IF-MIB values.

- CSCsj07297

Symptoms: Config sync is seen with Cisco 7600 HA routers.

Conditions: This symptom is observed when the **no vrrp 1 preempt** interface configuration command is configured and when a switchover is done from primary to secondary.

Workaround: There is no workaround.

- CSCsj27183

Symptoms: H323-->SIP interworking fails for a fast start call when transcoding is enabled on an IPIPGW. Transcoding is done between G711ulaw and G729r8 codecs.

Conditions: This failure is seen for H323--SIP--SIP--SIP and H323--SIP--SIP-- H323 call flows when transcoding is enabled on IPIPGW1. It is also seen on a H323--H323--H323--SIP call flow for transcoding on IPIPGW2. This is seen only with a fast start call (both with H245 Tunnel enabled and disabled), and the call passes with a slow start call.

Workaround: There is no workaround.

- CSCsj37071

Symptoms: All E1 interfaces on a PA-MC-E3 port adapter may flap continuously even after the traffic has been stopped.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a PA-MC-E3 port adapter when you configure 16 or 128 channel groups on each time slot (that is, time slots 1-31) and then generate traffic just above line rate traffic through all the channel groups. Note that the symptom is not platform-specific.

Workaround: Stop the traffic and reset the E3 controller of the PA-MC-E3 port adapter.

- CSCsj37709

Symptoms: Memory held by mem_mgr_chunk_t and mem_mgr_mempool_t in dead process is causing an out-of-memory condition on the gateway.

Conditions: This scenario occurs when SIP phone calls are made using the default application or a TCL IVR application and the **header-passing** command is enabled in voice service VoIP SIP configuration mode.

The following processes are the cause of the large amount of holding memory in *Dead* process:

```
0x61EC066C mem_mgr: mem_mgr_chunk_t 0x61EC091C mem_mgr: mem_mgr_mempool_t
```

Workaround: Disable the **header-passing** command.

- CSCsj38829

Symptoms: When running double authentication crypto (ah encap and esp encap auth together) configurations and passing large packet data which requires fragmentation, errored packets can be observed.

Conditions: This symptom has been observed only on routers with AIM-VPN-PLUS AIM cards installed. Routers which support this AIM are the Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 routers.

Workaround: Do not use ESP and AH double authentication. You can use the **no crypto engine accel** command in the configuration to run encryption in the SW engine.

- CSCsj50773

Symptoms: Performing the **snmpwalk** on the ipRouteTable MIB may cause high CPU and reloads.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

Workaround: Create a view that excludes the ipRouteTable:

```
snmp-server view cutover 1.3.6.1.2.1.4.21 exclude
snmp-server view cutover internet included
snmp-server community <comm> view cutover RO
```

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

- CSCsj54837

Symptoms: A Cisco 7200 that is running Cisco IOS Release 12.4 or 12.4(11)T2 crashes with a TLB (store) exception.

Conditions: This symptom is observed when Rate Based Satellite Control Protocol (RBSCP) tunneling is configured on the device.

Workaround: There is no workaround.

- CSCsj55043

Symptoms: On a Cisco 3800 router platform (Cisco 3825 or Cisco 3845), if multiple subinterfaces are configured on a Gigabit Ethernet motherboard interface and if these subinterfaces are configured with HSRP and the same VMAC, then whenever the router becomes HSRP standby for at least one of these subinterfaces, the router drops all traffic that is directed to the same VMAC on other subinterfaces.

The following is a sample configuration that would be exposed to this issue:

```
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 12.1.0.100 255.255.0.0
 standby 1 ip 12.1.0.1
 standby 1 mac-address 0000.0000.0001
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 12.2.0.100 255.255.0.0
 standby 2 ip 12.2.0.1
 standby 2 mac-address 0000.0000.0001
```

Conditions: This symptom is observed *only* on Cisco 3800 motherboard Gigabit Ethernet interfaces. It is not observed on Fast Ethernet/WAN modules or on other router platforms.

Workaround: The problem does not occur if different VMAC addresses are configured on different subinterfaces or if static VMACs are not used.

If the problem is encountered in a production environment, a quick workaround is to shut down the Gigabit Ethernet interface of the other router in order to make one router HSRP active in all VLANs.

- CSCsj58796

Symptoms: No ringback is generated in calls from VoIP to a PBX end using Cisco Multicast Manager (CMM).

Conditions: This symptom has been observed when a call is made from the VoIP side to the PBX side through an MGCP-controlled CMM.

PBX <-----GW (CMM or Cisco 2620XM) <----CCM <----IP Phone

Workaround: Use a Cisco 2620XM router in place of CMM.

- CSCsj58969

Symptoms: Executing the **show port modem calltracker** command on a Cisco AS5400XM can cause a bus error crash.

Conditions: This symptom occurs on a Cisco AS5400XM with multiple calls being made and terminated when running Cisco IOS Release 12.4(13a).

Workaround: There is no workaround.

- CSCsj64230

Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

Workaround: There is no workaround.

- CSCsj72647

Symptoms: On a Cisco IOS voice gateway, the **show call active voice brief** command output on the IP leg shows rx counters stay at 0 for 46 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7e).

Workaround: There is no workaround.

- CSCsj81722

Symptoms: A static address may have an aggregate out label in the BGP and MPLS forwarding entry.

Conditions: This symptom is observed when there is a static route in a VRF, a directly connected network is added, and both the static and connected routes are redistributed to BGP. The BGP table will then have the connected prefix, and both the BGP and forwarding entries will match and have the aggregate out label. But when the connected network is shut down, BGP gets the static route, but the out label remains "aggregate."

Workaround: There is no workaround.

- CSCsj87522

Symptoms: RTP and RTCP ports are leaked when a ReleaseComplete (reason=newConnectionNeeded) is received as a response to a FastStart Setup that is sent.

Conditions: This problem is seen in Cisco IOS Release 12.4(11)T and Release 12.4(15)T images for a normal H323 to H323 Gatekeeper routed call with no supplementary services.

Workaround: There is no workaround.

- CSCsj88665

Symptoms: A device with a PA-MC-2T3+ may reset because of a bus error if a channel group is removed while the **show interface** command is being used from another telnet session at the same time, and then the telnet session is cleared.

The device may also display Spurious Memory Accesses.

Conditions: These symptoms have been observed in the latest Cisco IOS 12.4T and 12.2S releases.

Workaround: Do not remove a channel group while using the **show interface** command for that interface.

- CSCsj88961

Symptoms: SNASwitch HPR/IP (Enterprise Extender - EE) receiving retransmissions due to HPR/IP UDP packets being dropped at the UDP socket layer in the SNASw router. This leads to poor throughput across the HPR/IP pipe.

Conditions: This can occur when receiving large bursts of HPR/IP traffic inbound to the SNASwitch router. The UDP socket inbound queue can hold a maximum of 50 packets. If more than 50 HPR/IP packets are received before the SNASwitch process can run and dequeue some, subsequent packets will be dropped.

Workaround: There is no workaround.

Further Problem Description: The output of the **show ip socket detail** command will show the number of drops that have occurred, the maximum queue size(50), and the highwater value. HPR/IP uses ports 12000 through 12004. Here is an example of UDP port 12003 showing 190577 dropped inbound packets:

```

Proto    Remote    Port      Local      Port      In      Out      Stat      TTY      OutputIF
  17    --listen--          x.x.x.x    12003      0        0        61        0
Queues:  output 0
          input 0 (drops 190577, max 50, highwater 50)

```

Resolution Summary: The resolution of this bug adds a new **qsize** parameter on the **snasw port** configuration command. This allows the specification of a UDP socket queue size value for HPR-IP ports only.

For example:

```
snasw port EE hpr-ip GigabitEthernet0/1 qsize 500
```

Note that the default of 50 was not changed by this. In order to increase the size of the UDP socket queue, the new parameter must be specified.

Other parameters may need to be adjusted as well:

Global configuration:

```
ip spd queue max-threshold 512 ip spd queue min-threshold 500
```

Under each IP interface where HPR/IP packets are flowing in and out of this router, add:

```
hold-queue 500 in
ip spd queue max-threshold 512 ip spd queue min-threshold 500
```

- CSCsj94561

Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot slot-number stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

Conditions: This symptom is observed on a Cisco 7200 series.

Workaround: There is no workaround.

- CSCsj95534

Symptoms: High CPU is observed on SNMP Engine while polling dsx1FracIfIndex for DS3s.

Conditions: This has been observed on a Cisco 7206 VXR platform having NPE-G1 that is running Cisco IOS Release 12.4(14).

Workaround: Applying a view on DS1 MIB prevents such high CPU usage. This prevents the user to monitor those entries.

Further Problem Description: The SNMP Engine comes into a loop and Get-NEXT always reports the same values. This happens while coming to the first interface channelized E3 card. Deleting this interface created the problem on the channelized E3 one.

- CSCsj95947

Symptoms: The following message is seen on the router:

```
*Aug 6 16:34:47.188: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC=
0x8005EC50, -Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50 0x800651E4
0x800652A8 0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0 0x809E42D4 0x80A0854C
0x800DB8C0 0x800DEE48
```

Conditions: The conditions under which this symptom occurs are not known at this time.

Workaround: There is no workaround.

- CSCsj96577

Symptoms: A Cisco AS5400HPX crashes due to a bus error as indicated by the following **show version** output:

```
System returned to ROM by bus error at PC 0x61728370, address 0xB0D0B45
```

Just before the crash, the following error message is seen:

```
%SYS-2-NOTQ: unqueue didn't find 674D6D40 in queue 3C -Process= "MGCP Application",
ipl= 0, pid= 170
```

Conditions: This symptom is observed on a Cisco AS5400HPX.

Workaround: There is no workaround.

- CSCsj97045

Symptoms: While running a Cisco IOS Release 12.4 Mainline release, a Cisco router may crash with a bus error. The error displayed will be similar to the following:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x605AFF94
```

Conditions: This symptom has been observed only if the gateway is configured for Voice over IP (VoIP).

Workaround: There is no workaround.

- CSCsj97602

Symptoms: A Cisco access server may run out of free processor memory. This symptom can be seen in the **show process memory** command. Increased memory utilization will be seen in the Dead pool.

Conditions: This symptom has been observed only in access servers that participate in Cisco Customer Voice Portal (CVP).

When a VXML application is configured with fetchaudio, the fetchaudio playout fails after user disconnect. The fetchaudio should have been removed from the prompt list, but it was not. This causes the session not to be freed when the application is finished.

Workaround: A reload will temporarily free the leaked memory.

- CSCsk00177

Symptoms: GRE traffic needs to be specifically allowed in the outside interface terminating DMVPN IPsec protected traffic.

Conditions: This symptom is observed on a DMVPN tunnel interface with tunnel protection IPsec, with CEF or fast switching.

Workaround:

- Use process switching.

- Allow the GRE traffic.
- CSCsk04970

Symptoms: There is a memory leak and fragmentation in *Dead* process due to MallocLite. After disabling malloclite, it will be seen as memory allocated to the “Virtual Exec” process in the **show memory allocating-process [total]** command output.

Conditions: The leak occurs whenever the **show vpdn session [l2tp] [all] username username** command is used, and there are many non-matching entries. Memory will be leaked proportional to the number of non-matching usernames (approximately 170 bytes per non-match).

Workaround: Avoid using the **show vpdn session [l2tp] [all] username username** command.
- CSCsk05059

Symptoms: A spurious access error occurs in `tfib_post_table_change_sanity_check ()` function.

Conditions: This symptom occurs if route is deleted. ROUTE_DOWN event is triggered in `tfib_post_table_change()` function which in turn calls `tfib_post_table_sanity_check()`. In that function, spurious access is reported, as the only path of route is down.

Workaround: There is no workaround.
- CSCsk05398

Symptoms: When a VXML application plays prompts and issues disconnect, the disconnect will be suspended until prompt playout completes. If the user hangs up before prompt playout completes, the disconnect event will not be thrown, and memory on VXML session will leak.

Conditions: This symptom is observed on a Cisco AS5400XM but is not platform dependent.

Workaround: There is no workaround.
- CSCsk09651

Symptoms: A router crashes while a service policy is being attached, detached, or modified across a virtual template under traffic.

Conditions: This symptom is observed on a Cisco 7200 or Cisco 7301 router that is configured with MLPPP over FR on channelized interfaces.

Workaround: There is no workaround.
- CSCsk09735

Symptoms: A router crashes when the **mkdir .../.../ EXEC** command is entered, followed by the **reload EXEC** command and the **show file system EXEC** command.

Conditions: This symptom is observed on a router that runs Cisco IOS software using a storage device that is formatted with the DOS file system.

Workaround: Avoid creating a subdirectory with “.” characters.
- CSCsk10133

Symptoms: During a mid-call codec switch from g.711 to g.729 on a gatekeeper-controlled gateway, the gateway may intermittently receive a Bandwidth Confirmation (BCF) message from the gatekeeper and wrongly detect it as a Bandwidth Reject (BRJ) message. This results in a release complete being sent from the gateway with a cause code of 65.

Conditions: This condition appears to be intermittent, due to the order of the OLC and the ECS (Empty Capability Set) messaging. This issue will be seen only on gatekeeper-controlled gateways that are doing bandwidth control. This issue is currently being seen only when codecs are switched mid-call to a codec with less bandwidth utilization.

Workaround: Any of the following workarounds should alleviate this issue:

1. Disable bandwidth requests from the gateway:
voice service voip h323 no ras brq
2. Configure all call legs to use the same codec.
3. Do not use a gatekeeper with this gateway.

Further Problem Description: This issue appears to be a recurrence of CSCee60960 and can be seen by enabling the following debugs:

- **debug h225 asn1**
- **debug ras**
- **debug cch323 all**

The following would be seen after the BCF is received:

```
581565: .Aug 15 13:45:06.376: //- 1/xxxxxxxxxxxxx/H323/cch323_ras_handle_rcv_msg:
received msg of type BCF_CHOSEN 581566: .Aug 15 13:45:06.376:
//94506/5A1D2CEFA2CC/H323/cch323_percall_ras_sm: ccb 0xC2A5CA58: received event
CCH323_RAS_EVENT_BCF while at CCH323_RAS_STATE_ACTIVE state 581567: .Aug 15
13:45:06.376: //94506/5A1D2CEFA2CC/H323/cch323_percall_ras_sm: ccb 0xC2A5CA58:
changing to new state CCH323_RAS_STATE_ACTIVE 581568: .Aug 15 13:45:06.376: //-
1/xxxxxxxxxxxxx/H323/cch323_iev_queue_service: Dispatch 0x1E internal event to H245
IWF SM 581569: .Aug 15 13:45:06.376: //94506/5A1D2CEFA2CC/H323/run_h245_iwf_sm:
received IWF_EV_BRJ while at state IWF_OLC_OUT_AWAIT_BCF 581570: .Aug 15
13:45:06.376: //- 1/xxxxxxxxxxxxx/H323/h323_set_release_source_for_peer:
ownCallId[94506], src [6] 581571: .Aug 15 13:45:06.376:
//94506/5A1D2CEFA2CC/H323/h245_iwf_set_new_state: changing from
IWF_OLC_OUT_AWAIT_BCF state to IWF_OLC_IDLE state 581572: .Aug 15 13:45:06.376: //-
1/xxxxxxxxxxxxx/H323/cch323_iev_queue_service: Dispatch 0xE internal event to H245 IWF
SM 581573: .Aug 15 13:45:06.376: //94506/5A1D2CEFA2CC/H323/run_h245_iwf_sm: received
IWF_EV_OLC_FAILED while at state IWF_ACTIVE 581574: .Aug 15 13:45:06.376: //-
1/xxxxxxxxxxxxx/H323/h323_set_cc_cause_for_spi_err: Categorized cause:65,
category:278
```

- **CSCsk10985**

Symptoms: IMA group interface does not come up after the reload.

Conditions: This symptom is observed on a Cisco 2811 router with ATM interface that is using VWIC2-2MFT-T1/E1 connected to MGX AUSUM card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface.

- **CSCsk16821**

Symptoms: A Cisco router acting as a DHCP server may experience the following problem when Secure ARP is also configured, and the Secure ARP keepalive time is less than the DHCP lease time. If a client device goes into sleep mode for a period of time less than the DHCP server's configured lease time but more than the Secure ARP time, the DHCP lease will be cancelled at the server. If the client awakes, it will have a valid DHCP lease, for the remainder of the last lease time it was granted. When the device awakes and attempts to renew its IP address, it sends a unicast DHCPREQUEST to the DHCP server. Because the lease has been removed from the DHCP server, and there is no ARP entry for the client, the DHCP Server does not send any reply to the device. The Secure ARP feature will, however, prevent the device from communicating until its lease has expired.

Conditions: This symptom has been observed with a Cisco router acting as a DHCP server when Secure ARP is also configured.

Workaround: Disable Secure ARP on the DHCP server or change the Secure ARP keepalive time to correspond to the lease time.

- CSCsk19661

Symptoms: In a Cisco 7500 HA router in RPR+ mode when configuring and unconfiguring channel groups under an E1 controller, the router reports the following:

```
*Aug 22 17:58:34.970: %HA-2-IPC_ERROR: Failed to open peer port. timeout *Aug 22
17:58:34.974: %HA-3-SYNC_ERROR: CCB sync failed for slot: 1 *Aug 22 17:58:34.974:
%HA-5-SYNC_RETRY: Reloading standby and retrying sync operation (retry 1).
```

and the standby RSP is reloaded.

Conditions: This symptom is observed when configuring and unconfiguring channel groups under an E1 controller.

Workaround: There is no workaround.

- CSCsk21209

Symptoms: A Cisco 7500 router may crash.

Conditions: This symptom occurs when dLFioFR and QoS are configured on the router and you try to move from dLFioFR to dLFioATM.

Workaround: There is no workaround.

- CSCsk25491

Symptoms: A Cisco router may reload and display a message similar to the following:

```
Aug 19 12:28:51.960: %SYS-3-MGDTIMER: Previous timer has bad forward linkage, timer
= 64176C30. -Process= "IPSEC key engine", ipl= 4, pid= 150 -Traceback= 0x607462F0
0x6084FD88
```

```
12:28:52 zulu Sun Aug 19 2007: Address Error (load or instruction fetch) exception,
CPU signal 10, PC = 0x60815DD4
```

Conditions: This symptom has been experienced on a Cisco 7206VXR that is running Cisco IOS Release 12.4(16).

Workaround: There is no workaround.

- CSCsk33780

Symptoms: Compressed Real-Time Protocol (cRTP) shows errors and Low Latency Queuing (LLQ) shows drops from default queue although there is no traffic to match it.

Conditions: This problem can be seen under load of MPPP bundle of several serial interfaces with LLQ and cRTP enabled.

Workaround: There is no workaround.

- CSCsk34832

Symptoms: Memory leaks out at about 10 to 15 percent overnight.

Conditions: This symptom occurs when a mix of application traffic is sent to the HTTP Secure server and when CPU utilization is at about 30 percent.

Workaround: There is no workaround.

- CSCsk35804

Symptoms: A Cisco router may experience a bus error crash preceded by the following error message:

```
%HMM_ASYNC-4-NO_MODEMS_PRESENT: HMM Digital Modem Card 1 contains no active modems
```

Conditions: This symptom is seen if the router contains a Digital Modem Network module that contains no SIMMs.

Workaround: Remove the card or install an NM-xDM card with valid SIMM modules.

- CSCsk36559

Symptoms: When one of the T1 or E1 controller NM-HDV2 goes down, the voice calls in the other controller are dropped.

This condition relates to interface x/0 x/0/0 (for example, 4/0 causes 4/0/0 to go down).

Conditions: This problem could happen in the MGCP PRI backhauled setup with NM- HDV2.

Workaround: There is no workaround.

- CSCsk42759

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsk42985

Symptoms: On a 1841/WIC-1/WIC-1B-U-V2/c1841-adventerprisek9-mz.124-13c combo [hereafter UUT], 180s after BRI interface successfully dials HUB PRI, 1/2 PING packets FAIL from HUB routers destined through UUT to a device on FastEthernet of the UUT, through the CEF switching path.

180 seconds after the ISDN Call from UUT successfully dials HUB PRI, "show adj vi1 internal" changed from point2point(21) to point2point(20) (incomplete) which coincides exactly with the PING failure. It also coincides with the CEF refresh timer triggering.

The direction of the failure is UUT-->HUB router with packets being dropped as "encapsulation failed" in "show ip traffic".

Conditions: Issue's been reproduced on 1841/WIC-1/WIC-1B-U-V2 using legacy DDR on BRI interface. Issue also reproducible in 124-16.14 IOS.

Issue is NOT reproducible on 1720/WIC-1B-U/c1700-sy-mz.122-40 combo.

Workaround: Disable CEF switching by configuring "no ip route-cache cef" on BRI0/1/0 and Fa0/1 on "nhstest2".

- CSCsk56496

Symptoms: On a router using high availability route processor redundancy (RPR)+, after an encapsulation change is done on serial interfaces of channelized port adapters, a reload of the slave Route Switch Processor (RSP) occurs.

Conditions: This symptom occurs when you exit configuration mode.

Workaround: There is no workaround.

- CSCsk57730

Symptoms: The **show flash / dir** commands throws an error message.

Conditions: This symptom has been observed only in certain versions of 5x routers Cisco AS5400XM and AS5350XM product running with a Cisco IOS Release 12.4(17.7) image.

Workaround: There is no workaround.

- CSCsk60020

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

- CSCsk62253

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

- CSCsk64021

Symptoms: A VXML gateway intermittently fails to submit a recording.

Conditions: This symptom is observed in Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCsl30214

Symptoms: A router crashes at function ether_oam_pd_shim_registry_init when the **ssg vc-service-map** command is configured.

Conditions: This symptom is observed on a Cisco 7200 series router that is loaded with Cisco IOS Release 12.4(18.4)T.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsh92986

Symptoms: The latency for the **RSH** command could increase when they are flowing through an FWSM module.

Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3, which is not affected by this extra delay issue.

- CSCsi33626

Symptoms: One may intermittently see a traceback from the Transport Port Agent because of timing of subsystem initialization in the router. The traceback is nonimpacting to the actual functional performance of the router.

Conditions: This symptom is observed at bootup.

Workaround: There is no workaround.

Wide-Area Networking

- CSCsi72045

Symptoms: A bus error crash occurs on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

Conditions: This symptom is seen with AAA and PPPoE configured.

Workaround: There is no workaround.

- CSCsj45148

Symptoms: Display IE contained in connect message is not passing through ISDN- to-H323 interworking at Originating Gateway (OGW).

Conditions: This happens when call Initiator makes a voice call to Path Terminating Equipment (PTE) (PC simulating remote-device) passing through VGW and OGW having Cisco IOS interim Release 12.4(16.9) images.

Workaround: There is no workaround.

- CSCsj47705

Symptoms: An accounting record may indicate that the NAS-Port-Id has an adapter number of 1 when the correct adapter number is greater than 1.

Conditions: This symptom is observed when AAA accounting is configured and a PPP interface that is used as a NAS port has more than two adapters.

Workaround: There is no workaround.

- CSCsk04350

Symptoms: When there are burst L2TP session authentication failures on the LNS and the **vpdn logging** global configuration is enabled, the system takes too many CPU cycles to print the syslog messages to the system console.

Conditions: Burst L2TP LNS session authentication fails.

Workaround: Disable system console logging by entering the **no logging console** global configuration command.

- CSCsk12238

Symptoms: Calls are torn down within a second after establishment.

Conditions: This symptom occurs when pinging from the client to the NAS gives the following:

```
Request drop link from bundle
```

Workaround: Configure the **dialer idle-timeout 0** command under the template. This will never bring down the calls nor bring down the physical link.

```
template template1
dialer idle-timeout 0
```

- CSCsk21431

Symptoms: A ping from the FR-DTE to the FR-DCE fails when FR-VCB is configured in the FR-DTE.

Conditions: This symptom is observed in Cisco IOS Release 12.4(16.14c).

Workaround: There is no workaround.

- CSCsk65172

Symptoms: MLP fails to negotiate MRRU when changing the default MTU (1500 bytes) configuration of multilink interfaces on the client, LAC, and LNS.

Conditions: This problem is seen only in a VPDN scenario with a Cisco IOS Release 12.4(17) image.

Workaround: There is no workaround.

- CSCsl11743

Symptoms: Multilinks are down after a switchover.

Conditions: This symptom is observed when dMLP and RPR+ are configured on a Cisco 7500 router and a switchover occurs.

Workaround: Micro-reload the Cisco 7500 router.

Resolved Caveats—Cisco IOS Release 12.4(17b)

Cisco IOS Release 12.4(17b) is a rebuild release for Cisco IOS Release 12.4(17). The caveats in this section are resolved in Cisco IOS Release 12.4(17b) but may be open in previous Cisco IOS releases.

- CSCek75633

Symptoms: A router may crash resulting in service impact.

Conditions: This symptom is observed on a Cisco 7200 router with NPEG2 when you attach a VC class to an ATM bundle. This is platform-independent. On other platforms a crash will not occur only traceback errors are noticed

Workaround: There is no workaround.

- CSCsg16778

Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

Workaround: There is no workaround.

Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- CSCsh22725

Symptoms: Outbound calls fail on a MGCP-controlled CAS channel on a Cisco VoIP gateway.

Conditions: This symptom is observed when the following conditions occur:

- A timeslot on an E&M T1 trunk is taken out of service from the connected switch side, showing as a permanent inbound seizure. In this situation, the output of the **show voice call summary** command indicates that the status for this channel is “EM_PARK”.
- A Cisco CallManager that interworks with the Cisco VoIP gateway checks the status of the trunk via an MGCP AUEP command. The gateway responds with an “ES: rlc” message, which indicates that the trunk is available for calls.

Because the reported availability and actual availability of the channel are mismatched, all outbound calls on the channel fail.

Workaround: Attempt to clear the out-of-service state from the connected switch side. If this is not possible, when interworking with the Cisco CallManager, first enter the **shutdown** command followed by the **no shutdown** command on the voice port and then enter the same commands on the T1 controller. Doing so causes the gateway to send an NTFY message that indicates that there is an inbound seizure on the channel.

- CSCsi20225

Symptoms: Continuous tracebacks may be generated on an LNS.

Conditions: This symptom is observed when you bring up PPPoX or L2TP sessions over multiple tunnels without traffic being processed over these sessions.

Workaround: There is no workaround.

- CSCsi29174

Symptoms: On a Cisco IOS voice gateway, the tx and rx counters in the output of the **show call active voice brief** command may not function properly. The counters may not increment at all or may increment in bursts every 10 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7c), Release 12.4(7d), Release 12.4(8c), or Release 12.4(13a).

Workaround: There is no workaround.

- CSCsj09838

Symptoms: When the BGP session between a Route Reflector (RR) and PE router flaps, the RR may no longer send some routes to the PE router.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsi85222. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi85222>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **clear ip bgp * all in** command on the PE router to retrieve all routes from the RR.

- CSCsj46178

Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router in either global MGCP configuration or MGCP profile.

Workaround: Do not configure the **endpoint naming t3** command. Use t1 endpoint naming instead.

- CSCsj49255

Symptoms: If there is an ACL and DSCP being used for packet matching on class- map, only the first packet descriptor will get a match, and everything else will not. If DSCP is removed, the packet matching works again.

Conditions: This symptom is observed on a Cisco 7200 with ACL and DSCP with match all option.

Workaround: There is no workaround.

- CSCsj74812

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: Occurs when running show commands on an exec session that has been established through one of the integrated modems on a WIC-AM or WIC-2AM. This would only be seen on async cards with gt96k, hwic or pquicc drivers.

Workaround: There is no workaround.

- CSCsj89544

Symptoms: If a BGP keepalive message fails to be sent to a BGP peer because the transport link is down, the neighbor BGP peer does not accept any further keepalive packets even though TCP retransmits the failed message using a backup path. This eventually causes the BGP peer to go down because of holdtime expiration.

Conditions: This happens when TCP retransmissions occur on MPLS-enabled network. This is seen only when MPLS is configured on Catalyst 6500 or Cisco 7600.

Workaround: There is no workaround.

- CSCsj93012

Symptoms: A Cisco 7500 router may crash when QoS is enabled.

Conditions: Occurs when ATM and serial interfaces have QoS configurations as output/input policy and when peer is reloaded.

Workaround: There is no workaround.

- CSCsj96577

Symptoms: A Cisco AS5400HPX crashes due to a bus error as indicated by show version “System returned to ROM by bus error at PC 0x61728370, address 0xB0D0B45”.

Just before the crash the following error message is seen:

```
SYS-2-NOTQ: unqueue didn't find 674D6D40 in queue 3C -Process= "MGCP Application",
ipl= 0, pid= 170
```

Conditions: This symptom is observed on a Cisco AS5400HPX.

Workaround: There is no workaround.

- CSCsk09651

Symptoms: A router crashes while a service policy is being attached, detached, or modified across a virtual template under traffic.

Conditions: This symptom is observed on a Cisco 7200 or Cisco 7301 router that is configured with MLPPP over FR on channelized interfaces.

Workaround: There is no workaround.

- CSCsk21431

Symptoms: A ping from the FR-DTE to the FR-DCE fails when FR-VCB is configured in the FR-DTE.

Conditions: This symptom is observed in Cisco IOS Release 12.4(16.14c).

Workaround: There is no workaround.

- CSCsk25651

Symptoms: With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM)/CallManager and utilizing SRST functionality, when the IP phones are registered to the SRST router, the message-waiting indication (MWI) states may be incorrect.

Conditions: When a phone registers to a Cisco SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come, first-served fashion. The MWI state, however, is remembered from the previous registration that used that ephone-dn number so the MWI status could be incorrect.

Workaround: Configure both the SRST router and the CUE to use SUBSCRIBE/NOTIFY MWI method.

- CSCsk26774

Symptoms: Native VLAN information is not included in CDP packets going out ports of an EtherSwitch (ESW) module in Cisco 28xx and Cisco 38xx routers. All the platforms using switchports (of any kind built-in/NM/WIC/HWIC) have this issue: Cisco 8xx, Cisco 17xx, Cisco 18xx, Cisco 26xx, Cisco 36xx, Cisco 37xx, Cisco 28xx, and Cisco 38xx.

Conditions: This symptom causes Cisco IP phone models 7961, 7941 and 7970 that are running SCCP firmware to fail to forward traffic coming from a PC connected at the back of the phone.

Workaround: Enable the “Voice VLAN Access” setting on the phone.

- CSCsk27147

Symptoms: The following SNMP is incorrectly generated:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
This issue is affecting the CISCO-MEMORYPOOL-MIB instead.
```

Conditions: Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because the input queue is full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

Workaround: Exclude ciscoMemoryPoolMIB from your query with the following commands:
snmp-server view public-view iso included snmp-server view public-view ciscoMemoryPoolMIB excluded Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

- CSCsk39642

Symptoms: A router crashes.

Conditions: This symptom is observed when you are running Cisco IOS Release 12.4(17) or Release 12.4T and when you copy the saved configuration to the running configuration.

Workaround: There is no workaround.

- CSCsk42759

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsk61790

Symptoms: Syslog displays password when copying the configuration via FTP.

Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

Workaround: There is no workaround.

- CSCsk62253

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

- CSCsk73104

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

- CSCsk88637

Symptoms: OAM cells are not generated when a new ATM subinterface and PVC is configured. Check subinterface and PVC status and enable the **debug atm oam interface atm/x.xxx** command. Subinterface will be up/up. PVC will be down, and no debug output will be seen.

Conditions: This symptom has been seen in various Cisco IOS 12.4 images.

Workaround: Perform **shut/no shut** commands on ATM subinterface.

- CSCsk94179

Symptoms: When IPv6 prefix delegation (PD) assigns a prefix for virtual access, it create a static route for the prefix in the routing table. However, sometimes it creates incorrect static route for the prefix. Conditions: The problem is observed when IPv6 PD is configured as a L2TP LNS.

Workaround: There is no workaround.

- CSCsk97384

Symptoms: Abnormally large FreshTime value appears in IVR HTTP client cache entry.

Conditions: This symptom is observed when a VXML voice browser downloads a file from an HTTP server. If the file was modified very recently, the FreshTime for that file may show up with a very large value.

Workaround: There is no workaround.

- CSCsl08480
Symptoms: Incoming traffic causes the following memory allocation failure: atm_vpivci_to_vc.
Conditions: Occurs on Cisco 7200 series routers.
Workaround: There is no workaround.
- CSCsl14635
Symptoms: T38 negotiation is failing for an incoming UPDATE request that has a T38 offer.
Conditions: This symptom occurs when the voice gateway is running Cisco IOS Release 12.4(15)T and is processing incoming Session Initiation Protocol (SIP) calls. When the SIP call is active and an UPDATE request is received that contains a T38 offer, the UPDAE request is rejected. The switchover from voice to fax fails.
Workaround: Fax over T38 works fine when midcall INVITE is used for T38 negotiation.
- CSCsl21123
Symptoms: Entering the **dir stby-harddisk:** command causes the active RP to crash.
Conditions: Occurs on a Cisco 7600 router.
Workaround: There is no workaround.none
- CSCsl24858
Symptoms: Cisco 7200 router with PA-VXC/B may go into “hang” state and fail to respond to console.
Conditions: Occurs on a Cisco 7200 router with PA-VXC/B and configured for active calls over the PA.
Workaround: There is no workaround.
- CSCsl32408
Symptoms: SIP gateway does not pass privacy information to the ISDN leg.
Conditions: The voice gateway is running Cisco IOS Release 12.4(15)T and processing incoming session initiation protocol (SIP) calls. When a SIP message is received on the voice gateway with calling number containing non-digit (calling number preceded by a '+'), then octet_3a information present in the SIP message is not passed to the ISDN leg.
Workaround: There is no workaround.
- CSCsl34303
Symptoms: Cisco 7200 router crashes when unconfiguring service policy from Multilink Frame Relay (MFR) interface.
Conditions: Occurs if one of the MFR bundle link interfaces was previously being used for Multilink PPP over Frame-relay. Changing the encapsulation may not clean up queuing configuration properly - a dual first in first out (FIFO) queue may remain on the interface.
Workaround: Ensure a dual FIFO queue is not present on MFR bundle link interface. It should be plain FIFO queue. If it is a dual FIFO, change the interface to HDLC encapsulation, which should remove the dual FIFO queue, then back to MFR bundle link encapsulation.
- CSCsl43394
Symptoms: Standby RSP reloads and has problems syncing configuration when DS1 controller is removed from DS3 configuration.
Conditions: This problem is seen when SSH is enabled on the router and DS1 controller is added or deleted from the configuration.

Workaround: There is no workaround.

- CSCsl62609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsl70143

Symptoms: Under heavy traffic, ISDN calls may be rejected due to high CPU usage with the following messages seen in the log (with tracebacks):

```
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (98/100). Call (callID=23524) is rejected.
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (32/18),process = ISDN.
```

Conditions: This problem occurs only under heavy traffic.

Workaround: There is no workaround.

- CSCsl71540

Symptoms: Router reloads when the **sh ip bgp options** command is entered.

Conditions: This is seen in releases where CSCsj22187 is resolved.

Workaround: There is no workaround.

- CSCsl87400

Symptoms: H323 setup message is malformed after NAT translation

Conditions: Setup message includes the neededFeatures, desiredFeatures, supportedFeatures extensions.

Workaround: Do not use the extensions listed above.

- CSCsl92595

Symptoms: After 3 minutes of normal operation, packet loss occurs over Dialer PPP multilink (MLPPP enabled) interfaces.

Conditions: Occurs when CEF is enabled and “ip address negotiated” is configured on the interface.

Workaround: Use one of the following options: Permanent: disable CEF with the **no ip cef** command. Permanent: configure a static IP address on the interface. Temporary: Use the **clear adj** command to refresh all adjacencies (will last 3 minutes).

- CSCsm04442

Symptoms: Delete an interface which has ip summary-address rip configured. The router crashes.

Conditions: In the scenario where different summary addresses are configured for different interfaces, if we delete an interface that has a summary-address configuration which is the last one for that summary-address that it leads to.

Workaround: Remove the **ip summary-address rip** configuration from an interface which is going to be deleted.

- CSCsm08291

Symptoms: Virtual access interfaces flap, and the following error message is displayed:

%SYS-2-BADSHARE: Bad refcount in datagram_done.

Conditions: Occurs on a Cisco 7206VXR with NPE-G2 and running Cisco IOS Release 12.4.(11)T1.

Workaround: There is no workaround.

- CSCsm20351

Symptoms: AAL2 trunk alarm is not generated for a resource availability indication (RAI) condition when a T1 is disconnected from a VWIC module.

Conditions: This issue is seen when AAL2 trunking is configured on a Cisco 2811 running Cisco IOS Release 12.4(17a)

Workaround: There is no workaround.

Further Problem Description: This issue is not seen on non-ISR platforms running Cisco IOS Release 12.3.

- CSCsm27726

Symptoms: After overwriting DHCP pool and client pool, status of client is IDLE.

Conditions: Occurs on Cisco routers running a pre-release version of Cisco IOS Release 12.4(17b).

Workaround: There is no workaround.

- CSCsm45113

Symptoms: Router may install duplicate routes or incorrect route netmask into route table. It could happen on any routing protocol. The problem is introduced by CSCsj50773. See the Integrated-in field of CSCsj50773 for affected images.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The **clear ip route *** command can restore the route table until next polling of ipRouteTable MIB.

Workaround: Do not poll ipRouteTable MIB. Instead poll newer replacement MIB, ipForward MIB. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Resolved Caveats—Cisco IOS Release 12.4(17a)

Cisco IOS Release 12.4(17a) is a rebuild release for Cisco IOS Release 12.4(17). The caveats in this section are resolved in Cisco IOS Release 12.4(17a) but may be open in previous Cisco IOS releases.

- CSCek71877

Symptoms: IPv6 pings are not working when the **atm route-bridged ipv6** command is configured on the UUT.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(13.5)T images.

Workaround: There is no workaround.

- CSCsg91306

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsh92986

Symptoms: The latency for the **RSH** command could increase when they are flowing through an FWSM module.

Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3, which is not affected by this extra delay issue.

- CSCsi57927

Symptoms: A Cisco router running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 will show TCP connections hung in CLOSEWAIT state. These connections will not time out, and if enough accumulate, the router will become unresponsive and need to be reloaded.

Conditions: This symptom occurs on a Cisco router running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 when executing a **copy source-url ftp:** command and the FTP server fails to initiate the FTP layer (no banner) but does setup a TCP connection. This may occur when the FTP server is misconfigured or overloaded.

The CLI command will timeout, but will not close the TCP connection or clean up associated resources. The FTP server will eventually answer and timeout itself, and close the TCP connection, but the router will not clean up the TCP resources at this time either.

Workaround: Manually clear TCP resources using the **clear tcp** CLI command, referencing the **show tcp brief** command output.

- CSCsi76616

Symptoms: Ldap packet modified passing through NAT router causing ldap to fail.

Conditions:

Network Topology

=====

LDAP server----->(fa00)NAT Router(fa(01)-----LDAP client

The packet after the NAT router seems to have been fragmentedexpanded to two parts in ldap:

Case1 - LDAP failed without "no-payload"

=====

- case1_before_nat_router -----> NAT Router -----> case1_after_nat_router
- LDAP packet modified

Case2 - LDAP passed with "no-payload"

=====

- case2_before_nat_router -----> NAT Router -----> case2_after_nat_router
- LDAP packet unchanged

Workaround: There is no workaround.

- CSCsi77147

Symptoms: DTMF path confirmation is not received for a SIP call.

Conditions: This problem is due to an issue with the SIP state machine, which may result in an error along the lines of the following:

```
00:05:10: //-1/xxxxxxxxxxxx/SIP/Error/sipSPISipIncomingMsg: Invalid method for
(STATE_IDLE): ACK
```

The call state should not be IDLE.

Workaround: There is no workaround.

- CSCsi81891

Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

Workaround: There is no workaround.

- CSCsj27183

Symptoms: H323-->SIP interworking fails for a Fast start call when transcoding is enabled on an IPIPGW. Transcoding is done between G711ulaw and G729r8 codecs.

Conditions: This failure is seen for H323--SIP--SIP--SIP and H323--SIP--SIP-- H323 call flows when transcoding is enabled on IPIPGW1. It is also seen on H323--H323--H323--SIP call flow for transcoding on IPIPGW2. This is seen only with a Fast Start call (both with H245 Tunnel enabled and disabled), and the call passes with a slow start call.

Workaround: There is no workaround.

- CSCsj37709

Symptoms: Memory held by mem_mgr_chunk_t and mem_mgr_mempool_t in dead process causes out of memory condition on gateway.

Conditions: This particular gateway is experiencing processes that are hung which is causing the router to run out memory. The following process are the cause of the large amount of holding memory in “*Dead*” process.

```
0x61EC066C mem_mgr: mem_mgr_chunk_t
0x61EC091C mem_mgr: mem_mgr_mempool_t
```

```
show processes memory sorted
```

```
Processor Pool Total: 484160064 Used: 254251956 Free: 229908108
I/O Pool Total: 134217728 Used: 47334444 Free: 86883284
```

PID	TTY	Allocated	Freed	Holding	Getbufs	Retbufs
Process						
0	0	3019495976	1504649520	127947176	12460712	524800 *Dead*
0	0	155229820	23382748	122271508	0	0

```
*Init*
```

Workaround: Disable the **header-passing** CLI.

- CSCsj38829

Symptoms: When running double authentication crypto (ah encap and esp encap auth together) configurations and passing large packet data which requires fragmentation, error packets can be observed.

Conditions: This symptom has been observed only on routers with AIM-VPN-PLUS AIM cards installed. Routers which support this AIM are the Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 routers.

Workaround: Do not use ESP and AH double authentication. You can use the **no crypto engine accel** command in the configuration to run encryption in the SW engine.

- CSCsj39538

Symptoms: Router tracebacks and then crashes during deconfiguration (removal) of VRF. The following message was seen prior to crash:

```
-Process= "IP RIB Update", ipl= 3, pid= 68
-Traceback= 609538D8 60D1B8B4 612B2838 612588C8 61258CD4 6125E61C 6125ED04
6125EF30 61261CDC 6125A14C 61265A08 6126BE10 6097CF00 609547D8 609548B8

Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0x609538FC
```

Conditions: No specific conditions are known to cause this fault.

Workaround: There is no workaround.

- CSCsj45148

Symptoms: Display IE contained in connect message is not passing through ISDN-to-H323 interworking at Originating Gateway (OGW).

Conditions: This happens when call Initiator makes a voice call to Path Terminating Equipment (PTE) (PC simulating remote-device) passing through VGW and OGW having Cisco IOS interim Release 12.4(16.9) images.

Workaround: There is no workaround.

- CSCsj58796

Symptoms: No ringback is generated in calls from VoIP to a PBX end using Cisco Multicast Manager (CMM).

Conditions: This symptom has been observed when a call is made from the VoIP side to the PBX side through an MGCP-controlled CMM.

```
PBX <-----GW (CMM or Cisco 2620XM) <----CCM <----IP Phone
```

Workaround: Use a Cisco 2620XM router in place of CMM.

- CSCsj58969

Symptoms: Executing the **show port modem calltracker** command on a Cisco AS5400XM can cause bus error crash.

Conditions: This symptom occurs on a Cisco AS5400XM with multiple calls being made and terminated when running Cisco IOS Release 12.4(13a).

Workaround: There is no workaround.

- CSCsj64230

Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

Workaround: There is no workaround.

- CSCsj72039

Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

Workaround: Remove and reconfigure the **passive-interface** command.

First Alternate Workaround: Enter the **clear isis *** command.

Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

- CSCsj72647

Symptoms: On a Cisco IOS voice gateway, the **show call active voice brief** command output on the IP leg shows rx counters stay at 0 for 46 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7e).

Workaround: There is no workaround.

- CSCsj85065

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>.

- CSCsj88961

Symptoms: SNASwitch HPR/IP (Enterprise Extender - EE) receiving retransmissions due to HPR/IP UDP packets being dropped at the UDP socket layer in the SNASw router. This leads to poor throughput across the HPR/IP pipe.

Conditions: This can occur when receiving large bursts of HPR/IP traffic inbound to the SNASwitch router. The UDP socket inbound queue can hold a maximum of 50 packets. If more than 50 HPR/IP packets are received before the SNASwitch process can run and dequeue some, subsequent packets will be dropped.

Workaround: There is no workaround.

Further Problem Description: The output of the **show ip socket detail** command will show the number of drops that have occurred, the maximum queue size(50) and the highwater value. HPR/IP Uses ports 12000 through 12004. Here is an example of UDP port 12003 showing 190577 dropped inbound packets:

```

Proto      Remote      Port      Local      Port  In Out Stat TTY OutputIF
  17    --listen--          x.x.x.x    12003    0  0  61   0
Queues: output 0
        input  0 (drops 190577, max 50, highwater 50)

```

Resolution Summary: The resolution of this bug adds a new **qsize** parameter on the **snasw port** configuration command. This allows the specification of a UDP socket queue size value for HPR-IP ports only.

For example: **snasw port EE hpr-ip GigabitEthernet0/1 qsize 500**

Other parameters may need to be adjusted as well:

Global configuration:

- ip spd queue max-threshold 512
- ip spd queue min-threshold 500

Under each IP interface where HPR/IP packets are flowing in and out of this router add:

- hold-queue 500 in
- ip spd queue max-threshold 512
- ip spd queue min-threshold 500

- CSCsj95534

Symptoms: High CPU is observed on SNMP Engine while polling dsx1FracIfIndex for DS3s.

Conditions: This has been observed on a Cisco 7206 VXR platform having NPE-G1 that is running Cisco IOS Release 12.4(14).

Workaround: Applying a view on DS1 MIB prevents such high CPU usage. This prevents the user to monitor those entries.

Further Problem Description: The SNMP Engine comes into a loop and Get-NEXT always reports the same values. This happens while coming to the first interface channelized E3 card. Deleting this interface created the problem on the channelized E3 one.

- CSCsj97045

Symptoms: While running a Cisco IOS Release 12.4 Mainline release, a Cisco router may crash with a bus error. The error displayed will be similar to:

```

Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0x605AFF94

```

Conditions: This symptom has been observed only if gateway is configured for Voice over IP (VoIP).

Workaround: There is no workaround.

- CSCsk00177

Symptoms: GRE traffic needs to be specifically allowed in the outside interface terminating DMVPN IPSec protected traffic.

Conditions: This symptom is observed on a DMVPN tunnel interface with tunnel protection IPSec, with CEF or fastswitching.

Workaround:

- use process switching.
 - allow the GRE traffic.
- CSCsk04970

Symptoms: There is a memory leak and fragmentation in *Dead* process due to MallocLite. After disabling mallocite, it will be seen as memory allocated to the “Virtual Exec” process in the **show memory allocating-process [total]** command output.

Conditions: The leak occurs whenever the **show vpdn session [l2tp] [all] username username** command is used, and there are many non-matching entries. Memory will be leaked proportional to the number of non-matching usernames (approximately 170 bytes per non-match).

Workaround: Avoid using the **show vpdn session [l2tp] [all] username username** command.
- CSCsk05059

Symptoms: A spurious access error occurs in `tfib_post_table_change_sanity_check ()` function.

Conditions: This symptom occurs if route is deleted. ROUTE_DOWN event is triggered in `tfib_post_table_change()` function which in turn calls `tfib_post_table_sanity_check()`. In that function, spurious access is reported, as the only path of route is down.

Workaround: There is no workaround.
- CSCsk05398

Symptoms: When a VXML application plays prompts and issues disconnect, the disconnect will be suspended until prompt playout completes. If the user hangs up before prompt playout completes, the disconnect event will not be thrown, and memory on VXML session will leak.

Conditions: This symptom is observed on a Cisco AS5400XM but is not platform dependent.

Workaround: There is no workaround.
- CSCsk10985

Symptoms: IMA group interface does not come up after the reload.

Conditions: This symptom is observed on a Cisco 2811 router with ATM interface that is using VWIC2-2MFT-T1/E1 connected to MGX AUSUM card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface.
- CSCsk12238

Symptoms: Calls are getting teared down within a second after establishment.

Conditions: This symptom occurs when ping from client to NAS gives “Request drop link from bundle”.

Workaround: There is no workaround.
- CSCsk16821

Symptoms: A Cisco router acting as a DHCP server may experience the following problem when Secure ARP is also configured, and the Secure ARP keepalive time is less than the DHCP lease time. If a client device goes into sleep mode for a period of time less than the DHCP server's configured lease time but more than the Secure ARP time, the DHCP lease will be cancelled at the server. If the client awakes, it will have a valid DHCP lease, for the remainder of the last lease time it was granted. When the device awakes and attempts to renew its IP address, it sends a unicast DHCPREQUEST to the DHCP server. Because the lease has been removed from the DHCP server, and there is no ARP entry for the client, the DHCP Server does not send any reply to the device. The Secure ARP feature will, however, prevent the device from communicating until its lease has expired.

Conditions: This symptom has been observed with a Cisco router acting as a DHCP server when Secure ARP is also configured.

Workaround: Disable Secure ARP on the DHCP server or change the Secure ARP keepalive time to correspond to the lease time.

- CSCsk16904

Symptoms:

- NAT router fails H323 connection by ARP resolution failure which ARP request is triggered by H225/H245 packet.
- When the problem occurs, NAT router creates incomplete entry and sends unexpected ARP request for destination IP address instead of nexthop IP address whereas the destination prefix is not directly connected route. Therefore if next-hop router of NAT router disable proxy-arp, the packet forwarding fails.
- Ping to same destination is no problem when the problem occurs.

Conditions: This problem happens when

- Static NAT or dynamic NAT is configured.
- Nexthop router of NAT router disable proxy-arp.
- H323 terminal device try to call for another one over NAT router.

Workaround: Enable proxy-arp on nexthop router.

- CSCsk19661

Symptoms: In a Cisco 7500 HA router in RPR+ Mode when configuring and unconfiguring channel groups under an E1 controller, the router reports the following:

```
*Aug 22 17:58:34.970: %HA-2-IPC_ERROR: Failed to open peer port. timeout *Aug
22 17:58:34.974: %HA-3-SYNC_ERROR: CCB sync failed for slot: 1 *Aug 22
17:58:34.974: %HA-5-SYNC_RETRY: Reloading standby and retrying sync operation
(retry 1).
```

and the standby RSP is reloaded.

Conditions: This symptom is observed when configuring and unconfiguring channel groups under an E1 controller.

Workaround: There is no workaround.

- CSCsk35985

Symptoms: The system crashes when the **show ipv6 ospf lsdb-radix** hidden command is entered.

Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

- CSCsk36559

Symptoms: When one of the T1 or E1 controller NM-HDV2 goes down, the voice calls in the other controller are dropped.

This condition relates to interface x/0 x/0/0 (for example, 4/0 causes 4/0/0 to go down).

Conditions: This problem could happen in the MGCP PRI backhauled setup with NM-HDV2.

Workaround: There is no workaround.

- CSCsk42985

Symptoms: On a Cisco 1841-adventerprisek9-mz.124-13c combo [hereafter UUT], 180s after BRI interface successfully dials HUB PRI, 1/2 PING packets FAIL from HUB routers destined through UUT to a device on FastEthernet of the UUT, through the CEF switching path.

180 seconds after the ISDN Call from UUT successfully dials HUB PRI, “show adj vi1 internal” changed from point2point(21) to point2point(20) (incomplete) which coincides exactly with the PING failure. It also coincides with the CEF refresh timer triggering. The direction of the failure is UUT-->HUB router with packets being dropped as “encapsulation failed” in “show ip traffic”.

Conditions: This issue has been reproduced on Cisco 1841 using legacy DDR on BRI interface. This issue is also reproducible in Cisco IOS interim Release 12.4(16.14). The symptom is platform independent. The issue is not reproducible on Cisco 1720/WIC-1B-U/c1700-sy-mz.122-40 combo.

Workaround: Disable CEF switching by configuring “no ip route-cache cef” on BRI0/1/0 and Fa0/1 on UUT.

- CSCsk60020

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>

Resolved Caveats—Cisco IOS Release 12.4(17)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(17). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(17). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCei62358

Symptoms: The Cisco 805/rsp720 router with Cisco IOS Release 12.3(15)/12.2(33)SRB1 with crash when a privilege level 15 user logon with attribute "call-back".The AAA server is ACS 2.4.

Customer config call-back/callback-dialstring attribute for the user.If remove this attribute,there is no crash.

Conditions: This symptom has been observed with a Cisco 805/rsp720 router configured with AAA authentication and authorization. ACS server is 2.4. On ACS configuration, a user with callback attribute (customer also use this user as a dialin for Cisco AS5200). When this user try to logon, the Cisco 805/rsp720 router crashes.It happens repeatedly.

Workaround:

1. Do not configure the **call-back** attribute for the user.
2. Avoid to configure NULL value for the callback-dialstring attribute in the Tacacs+ profile.

- CSCek78644

Symptoms: SNMP does not use the source address in a VRF.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: Ensure that an SNMP interface is not defined in a VRF.

- CSCsi48665

Symptoms: When you configure SNMPv3 group access to contexts, each context may need to be configured with a separate CLI command. For large configurations, thousands of CLI command may need to be entered, which is not acceptable.

Conditions: This symptom is observed, for example, when the **snmp-server group groupname v3 auth context context-name** command must be entered for each group and each context. If there are many VLANs, the command must be entered for each group that is given access to each VLAN, which may mean that thousands of CLI command must be entered.

Workaround: SNMP allows you to specify that a context name is a prefix, and match any context that starts with that name. Use SNMP to create rows in the vacmAccessTable and ensure that the vacmAccessContextMatch object is set to a prefix instead of match. Note that after you reboot the router, you must reconfigure this workaround.

- CSCsi75545

Symptoms: Some of the RFC 2217 commands sent to the Cisco IOS may not be acknowledged i.e., the server may not respond back for certain commands.

Conditions: Clients using a RFC 2217 to talk to Cisco IOS to control a serial device will see this problem

Workaround: The only workaround is not to send these commands, but it may not be acceptable in all cases

- CSCsi77088

Symptoms: Error messages are getting displayed continuously and unable to get the router console.

Conditions: This symptom has been observed while loading image in Cisco 7500 series routers.

Workaround: There is no workaround.

- CSCsi96900

A Cisco port adaptor CT3IP-50 running Cisco IOS Release 12.0(32)S6 may reload unexpectedly. This has been experienced many times. The information gathered points to a software issue. This enclosure will be updated as more information is gathered.

CT3IP-50 w/ 128MB DRAM running Cisco IOS Release 12.0(32)S6 crashed due to:

```
%SYS-3-CPUHOG: Task ran for 123588 msec (2838/0), process = VIP Txacc loss
compensation, PC = 60308350.
-Traceback= 60308358 : %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process =
VIP Txacc loss compensation.
-Traceback= 60030DC4 6011774C 6011C244 6010EDF4 603081D0 6030851C
20:32:43 UTC Mon Apr 16 2007: Breakpoint exception, CPU signal 23, PC = 0x6010CF38
```

Conditions: This symptom has been observed with

Workaround: Enable “no service txacc-accounting” on the RSP.

Note: You may have to enter service internal first.

- CSCsj30317

Symptoms: FIBDISABLE seen on all VIPs on Cisco 7500 router.

Conditions: This symptom has been observed with: MLP+QoS is configured on Cisco 7500 router.

Workaround: There is no workaround.

- CSCsj55691

Symptoms: Crash on the router.

Conditions: For the problem to occur, there need to multiple https requests sent in quick succession to an HTTPS server that is up and running but the service or application processing the request should be unavailable.

Workaround: There is no workaround.

Further Problem Description: The crash will not occur if the HTTPS Server and the service handling the request are operating normally.

EXEC and Configuration Parser

- CSCse22016

Symptoms: The **show running** commands get cut if beyond a certain char limit.

Conditions: This symptom has been observed with truncated multilink interface numbers.

Workaround: There is no workaround.

Further Problem Description: Problem occurred because of a bad codefix to the nv_write_internal function which takes care of printing the proper characters into sh running.

IBM Connectivity

- CSCsi57284

Symptoms: A router that is running Cisco IOS may crash due to a software forced crash.

Conditions: This symptom has been observed with a DLSW configuration with SDLC attached controllers. At the time of the crash, on one SDLC interface, the encapsulation SDLC was removed.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCek76288

Symptoms: With MLPoATM configured router crashes on issuing <show ppp multilink> after disabling the PA by issuing <hw-module slot # stop>

Conditions: This symptom has been observed with a Cisco 7200 NPE-G1 loaded with Cisco IOS Release 12.4(13.13)T2 image.

Workaround: There is no workaround.

- CSCsi41769

Symptoms: A PVC that is shut down by OAM may continue to receive and forward traffic. This situation causes problems in an APS 1+1 redundancy configuration in which the standby router has a PVC that is shut down by OAM but continues to receive all traffic.

Conditions: This symptom is observed on a Cisco router that has an ATM port adapter.

Workaround: In an IPv4 configuration, shut down the subinterface manually or enter the **ip verify unicast reverse-path** command. In an MPLS configuration, shut down the subinterface manually.

- CSCsi56413

Symptoms: The output may be stuck on a POS interface that is configured for Frame Relay encapsulation. When this situation occurs, the output queue is not emptied, and LMI remains down.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(12) or later. This happens only with very specific hardware configurations including NPE-G1 and PA-POS-OC3SML. The issue observed when aforementioned Port Adapter is located at slot 4 and not seen with other hardware configurations.

Workaround: Place POS PA in other slot(s). PA location reconfiguration in chassis should fix the problem.

- CSCsi85935

Symptoms: Alignment errors drive the router to crash due to a bus error (TLB exception). These reloads can occur about 2-3 times day.

Conditions: This symptom has been observed with a Cisco 3745 with NM-8AM running Cisco IOS Release 12.3(7)T11 and 12.4(13a) while there is great volume of the traffic through module NM-8AM. Replacement of all the HW equipment didn't solve the issue.

Workaround: Reduce traffic through NM module or install Cisco IOS Release 12.3 (not T train or 12.4 image) provokes that reloads stop.

IP Routing Protocols

- CSCek47667

Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

Workaround: There is no workaround.

- CSCek76776

Symptoms: at big service provider whereas atm-sub interfaces are deleted and new one created on regular basis as they remove and add new end customers.

Because it is not a manual process as scripting is used to perform that task, old configuration from deleted sub-interface are showing up on new sub-interfaces and in some cases are creating outages.

Conditions: This symptom has been observed with Cisco IOS Release 12.0(27)S5d.

Workaround: verify sub-interface configuration and if configuration cannot be deleted on that sub-interface, delete this sub-interface then create a dummy sub-interface which will pull that configuration. Then recreate prior sub-interface.

- CSCek78315

Symptoms: Router may give spurious memory access or crash when the **debug ip ospf hello** command is enabled on the router, which has sham-links configured.

Conditions: This symptom has been observed with sham-links configured. Only Cisco IOS images with the fix CSCse35155 integrated are affected. The **debug ip ospf hello** command is enabled during the adjacency start on the sham-link interface.

Workaround: Do not start the **debug ip ospf hello** command in a sham-link environment.

- CSCsg07742

Symptoms: The attributes that are configured in a site map may not automatically be applied to the BGP table when the associated interface is running other routing protocols such as RIP or OSPF.

Conditions: This symptom is observed on a Cisco router when routes are redistributed into BGP.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the associated interface.

- CSCsg55591

Symptoms: When there are link flaps in the network, various PE's received the error msg %BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix 155:14344:10.150.3.22/32 from 10.2.2.1

OR

Local label is not programmed into forwarding table for a sourced BGP VPNv4 network

Conditions: This symptom has been observed when an iBGP path for a VPNv4 BGP network is present, then a sourced path for the same RD and prefix is brought up after.

Workaround:

- Remove the iBGP path. If the sourced path comes up first, then the problem will not occur
- Use different RDs with the different PEs. If the RD+prefix does not match exactly between the iBGP path and the sourced path, the problem will not occur.

- CSCsh14457

Symptoms: Cisco router running modular image (-vz- version) configured for OSPF and BFD may experience corner case crash.

Conditions: This symptom has been observed with a high number of very unstable OSPF/BFD neighbors.

Workaround: Upgrade to fixed software version.

- CSCsh53926

Symptoms: A router may crash because of a bus error in the OSPF process.

Conditions: This symptom is observed on a Cisco router that is configured for incremental SPF (ISPF) and that functions in a network with MPLS TE tunnels.

Workaround: Remove the ISPF configuration.

- CSCsh78277

Symptoms: An "Mwheel" CPU hog conditions may occur, and the platform may crash.

Conditions: This symptom is observed in a multicast configuration when an RPF link changes.

Workaround: There is no workaround.

- CSCsh82953

Symptoms: On a PE router in an EIGRP network, EIGRP prefixes are redistributed into BGP but are missing their EIGRP-derived extended community values.

Conditions: This symptom is observed only when a **network** command is manually entered in "router EIGRP" mode while the **redistribute eigrp** command already exists in the BGP configuration. The symptom does not occur if all final configuration statements are present at router bootup time.

Workaround: Re-enter the **redistribute eigrp** command in the BGP configuration. There is no need to first remove the command because entering the command triggers a new redistribution event.

- CSCsi16628

Symptoms: static NAT has memory leaking when configure "vrf route-map reversible extendable"
Router memory decreases dramatically when there is certain volume of tcp traffic.

Conditions: This symptom has been observed with Cisco IOS Release 12.4(9)T2 and Release 12.4(11)T1. This problem only happens when configured "route-map reversible" Normal static vrf NAT does not have this issue.

Workaround: There is no workaround.

- CSCsi32425

Symptoms: A router that is configured for static NAT translations may lose its external/global ARP entry for a NAT address.

Conditions: This symptom is observed when traffic flows run across the router, for example, when the client is outside and server is inside, and when static NAT translation is used for periods of about two minutes.

Workaround: Configure a route map that matches the static NAT translation, and apply the static NAT entry by entering either one of the following commands:

- **ip nat inside source static tcp local-ip local-port global-ip global-port route-map name reversible**

- **ip nat inside source static local-ip global-ip route-map name reversible**

- CSCsi33147

Symptoms: Prefix LSA does not get updated after interface un-shutdown.

Conditions: This symptom has been observed with

Workaround: There is no workaround. Bounce the interface again will fix the issue.

Further Problem Description: This is rare timing issue, so far it seen in a lab only when virtual link is configured.

- CSCsi35541

Symptoms: An CPUHOG may be experienced after executing command clear ip route *

Conditions: This symptom is observed with:

- many connected routes, CPUHOG seen with 1000+ subinterfaces.

- OSPF process which is not running, because it can not pick up a router-id.

Workaround: Avoid having configured OSPF process which can not start because no router-id is available.

- CSCsi42680

Symptoms: After a mapping ID has been removed from the Stateful NAT Translation (SNAT) global configuration, a SNAT router may crash unexpectedly.

Conditions: This symptom is observed on a Cisco router that functions as a SNAT router and that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: There is no workaround.

- CSCsi48304

Symptoms: The IOS error message:

```
%OSPFv3-3-DBEXIST: DB already exist
```

may be printed if OSPFv3 router redistributes large number of the external routes, usually after reload. So far no impact of the error message to the operation of the router has been experienced.

Conditions: This symptom has been observed with Redistribution configured and the router reloaded.

Workaround: Upgrade to not affected IOS version.

- CSCsi59438

Symptoms: When you enter the **ip multicast limit rpf** command, protection may fail after the RPF link becomes operational.

Conditions: This symptom is observed on a Cisco router that is configured for APS switchover.

Workaround: Clear the state of the corresponding multicast route by entering the **clear ip mroute** command.

- CSCsi62559

Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsi68882

Symptoms: A router running EIGRP can crash when removing an EIGRP process.

Conditions: The crash will only happen where there are more than thirty IP routing protocol processes created and the last one is EIGRP. Note that this does not include VRFs. When the 31st routing protocol process is attempted, an error message will be issued stating "too many IP routing processes". If attempt is then made to remove an EIGRP routing process by doing the command "no router eigrp <as>", the router will crash.

Workaround: Don't define over 30 IP routing protocol processes.

- CSCsi84089

Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

Workaround: Add area 0 in the OSPF VRF processes.

Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi86386

Symptoms: The **clear ip bgp * soft in** command does not function for an inbound route map.

Conditions: This symptom is observed on a Cisco router that has the **neighbor send-label** command enabled when the prefix that is being filtered is an IPv4 unicast prefix.

Workaround: Enter the **clear ip bgp *** command.

Further Problem Description: The **clear ip bgp * soft in** command does function fine for other address families such as VRF and VPNv4.

- CSCsi97586

Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

Workaround: There is no workaround.

ISO CLNS

- CSCek76093

Symptoms: A CLNS neighbor may still be formed after the IS-IS protocol has been shut down.

Conditions: This symptom is observed only on serial interfaces.

Workaround: There is no workaround.

- CSCsi41944

Symptoms: After redistribution-related configuration changes have been made, a CPUHOG condition may occur in the Virtual Exec process, causing loss of IS-IS adjacencies.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF when the **redistribute maximum-prefix** command is configured under the **router isis** command and when BGP is configured to be redistributed into IS-IS. The symptom could also affect a Cisco 7600 series router that runs Release 12.2SR.

Workaround: There is no workaround.

- CSCsi57971

Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database on a local router.

Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Miscellaneous

- CSCdz55178

Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
00000000011111111122222222333^ 12345678901234567890123456789012 | PROBLEM
(Variable Overflowed).
```

Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCeg20335

Symptoms: A Cisco 10000 series may lose the PVC configurations for several subinterfaces and high CPU usage may occur. When you attempt to reconfigure the PVCs, error messages similar to the following may be generated:

```
Router#pvc 35/134 Unable to create PVC 35/134 on ATM1/0/0.10350134. Possibly multiple users
configuring IOS simultaneously Further info about other user: Process id: 42, Process: Slot 1/0
CMD Process, TTY: 0, Location: Console Router(config-subif)#
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(7)XI1 or Release 12.2(27)SBB.

Workaround: Reload the router.

- CSCeh56808

Symptoms: The **ip auth-proxy** command may not take effect when it is configured on VLAN interfaces, and the following error message may be generated:

```
"Auth-Proxy not configured on interface FastEthernet0/0/0".
```

(This error message is generated when an IP phone is connected to port Fa0/0/0.)

Conditions: This symptom is observed only on a router that is configured with switchport interfaces.

Workaround: Configure the **ip auth-proxy** command on the ingress interface. If this is not an option because the **ip auth-proxy** command must be configured on VLAN interfaces, there is no workaround.

- CSCeh98127

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: The router must be configured for QoS.

Workaround: Disable QoS.

- CSCek49107

Symptoms: A router crashes when you unconfigure and then reconfigure MLPoFR.

Conditions: This symptom is observed on a Cisco router that has a QoS service policy with traffic shaping.

Workaround: There is no workaround.

- CSCek52234

Symptoms: A Cisco Gigabit Ethernet Interface goes down when set to speed 100 / Full Duplex and when the remote end is third party LAN extension service equipment.

Conditions: This symptom has been observed on Cisco 3800 Gigabit Ethernet interface. A Cisco 2811 FastEthernet interface or Cisco 2821 Gigabit Ethernet do not show the problem. The symptom is also not seen if a Cisco Catalyst 4506 is used in place of the third party equipment.

Workaround: Use hardware other than Cisco 3800 Gigabit Ethernet when connecting to third party equipment.

- CSCek74858

Symptoms: When the command "glbp <group> weighting track <track_number>" is configured on the Active processor of an HA capable router, the equivalent command does not get synced to the Standby processor config. This means that after processor switchover, the GLBP weighting track command will have no affect on the operation of the group.

Conditions: This symptom has been observed with HA capable routers in RPR, RPR+ or SSO mode, and supporting GLBP.

Workaround: There is no workaround for this issue. The config will have to re-entered into the new Active processor config after switchover.

- CSCin30349

Symptoms: Interface flaps on an ATM IMA port adapter may cause the router to reload.

Conditions: This symptom has been observed when using an PA-A3-8T1IMA/PA-A3- 8E1IMA port adapter on Cisco 7xxx series router platforms. Flaps must be observed or the **shutdown** and **no shutdown** commands must be performed on an applicable interface. However, this symptom is a rare condition, and will not necessarily occur with every flap. This symptom can occur with or without traffic.

Workaround: There is no workaround.

- CSCin33561

Symptoms: A Cisco switch or router may reload when you configure an ATM User-Network Interface (UNI) link on an ATM interface of an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA).

Conditions: This symptom is observed on a Cisco Catalyst 6000 series, Cisco 7500 series, and Cisco 7600 series when an ATM link is configured after the platform has booted up.

Workaround: There is no workaround.

- CSCsb15164

Symptoms: In Cisco IOS, when configuring a standard Access List host-level permit entry after a host-level deny entry, the order of ACL entries is reordered. In the running-configuration, the permit entry is placed at the top of the list. There is a chance packets will be permitted when they should be denied.

Workaround: Extended ACLs do not exhibit this behavior.

- CSCsc75199

Symptoms: An SCCP analog gateway crashes when using the auto-configuration feature under CCM 5.x control.

Conditions: This symptom has been observed when the SCCP auto configuration feature is enabled and the SCCP GW is under CCM 5.x control

Workaround: There are two workarounds:

1. Do not use the SCCP auto configuration feature. Instead configure analog end points on the GW via the CLI.
2. Use CCM 4.1.x or 4.2 release instead of CCM 5.x release.

- CSCsd09324

Symptoms: When reloading a router (lsnt-ap-pe1, Cisco 7500 platform) with Cisco IOS interim Release 12.0(31.4)S1 from any Cisco IOS Release 12.0(28)S4b image, several IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP and traceback occur in the standby log.

Conditions: This symptom has been observed on a Cisco 7500 router platform with MVPN.

Workaround: There is no workaround.

- CSCsd78518

Symptoms: When using vrf-aware DVTI, when a DF-set packet exceeds the IPSEC SA path MTU, the PMTUD ICMP unreachable packet sent from the Cisco 7206 router contains the correct originator IP address, but it is sourced incorrectly to the PVRF(FVRF) tunnel termination loopback instead of the CVRF(IVRF) loopback and it is forwarded incorrectly out the PVRF(FVRF) routing table instead of the CVRF(IVRF) routing table. This issue appears to also exist in Cisco IOS Release 12.4(4)T2. This issue will also appear if an IP MTU is set in the virtual-template configuration. If a IP MTU is set within the virtual-template and a DF-set packet is sent to the virtual-access interface that violates this MTU, a PMTUD ICMP unreachable message is forwarded correctly from the CVRF(IVRF) loopback to the originator as expected.

Conditions: This symptom has been observed with Example DVTI config:

```
interface Virtual-Template1000 type tunnel description cust1-h-g1 ip vrf forwarding cust1-u-p ip
unnumbered Loopback1001 tunnel mode ipsec ipv4 tunnel vrf pvr tunnel protection ipsec profile
cust1-h-g1-ips
```

IP ICMP and IP packet debug capture of incorrect ICMP packet:

```
*Mar 24 15:52:05.778: ICMP: dst (10.100.15.2) frag. needed and DF set unreachable sent
to 10.100.14.2
*Mar 24 15:52:05.778: IP: tableid=8, s=10.77.37.220 (local), d=10.100.14.2
(GigabitEthernet0/2), routed via FIB
*Mar 24 15:52:05.778: IP: s=10.77.37.220 (local), d=10.100.14.2 (GigabitEthernet0/2),
len 56, sending
*Mar 24 15:52:05.942: IP: tableid=0, s=10.3.0.43 (GigabitEthernet0/2), d=10.4.0.1
(Loopback0), routed via RIB
*Mar 24 15:52:05.942: IP: s=10.3.0.43 (GigabitEthernet0/2), d=10.4.0.1, len 40,rcvd 4
ACL trace of packet in downstream router from 7206's PVRF/FVRF:
```

```
Mar 24 23:00:14 UTC: %SEC-6-IPACCESSLOGDP: list mtul permitted icmp 10.77.37.220 ->
10.100.14.2 (3/4), 8 packets
```

Workaround: There is no workaround.

- CSCse55425

Symptoms: When configuring a Serial interface or issuing **show** commands related to that Serial interface, a router may incorrectly configure a different Serial interface or may show output from a different Serial interface in the router.

Conditions: The conditions under which the problem manifest itself are unknown, and appear to be random. The problem exists only when using a channelized T3 card and configuring one of the T1's.

Workaround: A router reload clears the issue.

- CSCse59336

Symptoms: MGCP three-way call conferencing may fail because of an abrupt onhook event at the originating endpoint.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) and that is configured for voice calls over Media Gateway Control Protocol (XGCP).

Workaround: There is no workaround.

- CSCse64750

Symptoms: "%VPA-3-TSBSY:VPA" and other error messages may be generated intermittently, and calls may fail.

Conditions: This symptom is observed on a Cisco 7206VRX that is configured with multiple VXC voice port adaptors.

Workaround: There is no workaround.

- CSCse76935

Symptoms: A router that is configured for SNA Switching Services (SNASw) may crash.

Conditions: This symptom is observed when links with an end node go down and when there are multiple links to the end nodes, at least one of which supports CP-CP sessions, and one of which does not. The symptom occurs on rare occasions because of a timing condition.

Workaround: Change the end node device configuration such that all links to the SNASw router support CP-CP sessions. As per the APPN architecture, only one link does actually support CP-CP sessions.

Further Problem Description: The symptom occurs because there is a mix of APPN links (that support CP-CP sessions) and LEN links (that do not support CP-CP sessions) from an end node to the SNASw router. The recommended configuration is to have all links between two partners be of the same type. Because LEN links generally do not support parallel TGs, most likely these should be APPN links, all supporting CP-CP sessions. This is a product-dependent configuration on the end node product.

- CSCse83545

Symptoms: A router may crash during the assignment of a MAC address for a virtual Token Ring interface.

Conditions: This symptom is observed when the virtual Token Ring interface is configured for IP Traffic Export.

Workaround: There is no workaround.

- CSCsf11944

Symptoms: Router crashes due to the stack for process Exec running low on configuring auto qos on an atm subinterface.

Conditions: This symptom has been observed with a router loaded with Cisco IOS Release 12.4(10.5).

Workaround: There is no workaround.

- CSCsg03739

Symptoms: A memory leak may occur in the "Crypto IKMP" process.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA (SPA-IPSEC-2G).

Workaround: There is no workaround.

- CSCsg42546

Symptoms: An MGCP gateway reloads when receiving Secure Real-Time Transport Protocol (SRTP) and V.150 parameters in the local connection options of a Create Connection (CRCX) message.

Conditions: This symptom has been observed when the gateway is configured to use SRTP and V.150 protocols.

Workaround: Disable the use of either SRTP or V.150 protocol in the gateway.

- CSCsg70474

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

- CSCsg71395

Symptoms: High CPU usage may occur in the "CCH323_CT" process on a gateway.

Conditions: This symptom is observed on a Cisco router that is configured as an H.323 gateway and that functions in the following topology:

IP Phone---CCM--- Incoming VoIP Dial Peer -- Cisco H.323 Gateway---FXS -- IVR

The "app-h450-transfer.2.0.0.9.tcl" application is applied on the incoming VoIP dial peer. The symptom occurs when IVR transfers the call and when the transferred call is put on hold.

Workaround: Enter the **clear call voice id *call-id*** command to clear the VoIP leg between the Cisco CallManager and the Cisco H.323 gateway. Doing so decreases the CPU usage. Obtain the Call ID from the output of the **show call active voice brief** command.

Alternate Workaround: Reload the router. Note, however, that high CPU usage may occur immediately after you have reloaded the router if the scenario that is described in the Conditions re-occurs.

- CSCsg84975

Symptoms: MGCP NAS calls are dropped

Conditions: This symptom has been observed when there is heavy E1 flaps.

Workaround: There is no workaround.

- CSCsg86036

Symptoms: A Cisco 2800 memory leak when receiving abnormal MGCP message continuously.

Conditions: This symptom has been observed with MGCP media gateway is enabled.

Workaround: There is no workaround.

- CSCsg92377

Symptoms: Packet drops due to interface throttles are seen on the GGSN R7.0 during performance test.

Conditions: The throttles seen when bi-directional traffic of 70 Mbps in the ratio of 1:4 upstream:downstream is sent over 60k ipv4 pdp's across 500 VRF Apn's. One throttle per minute was observed.

Workaround: There is no workaround.

- CSCsg99814

Symptoms: On a router that functions in a GRE over IPsec or Virtual Tunnel Interface (VTI) configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface.

Conditions: This symptom is observed when the ACL on the tunnel interface is configured on the outbound physical interface on which the IPsec tunnel is terminated.

Workaround: Apply the outbound ACL on the protected LAN interface instead of on the tunnel interface.

- CSCsh06117

Symptoms: When the ATM Software Segmentation and Reassembly (SAR) feature is enabled, VBR-rt PVCs may be deactivated before VBR-nrt PVCs in an over-subscription scenario.

Conditions: This symptom is observed on a Cisco 2600 series and Cisco MC3810 that have oversubscribed ATM PVCs with a VBR-rt and VBR-nrt class of service.

Workaround: Configure all PVCs with an SCR of less than or equal to the line rate.

- CSCsh20946

Symptoms: MWAM processor running as GGSN in a GTP-SR active/standby redundant system may encounter software exception during a failover.

Conditions: The exception is noticed under the following condition. - Create a few thousand IPv4 PDP contexts (e.g. 20000) on the MWAM GGSN processor. - Reset the active-GGSN MWAM module. The MWAM GGSN in the other chassis as standby will now become active. - When the reset MWAM boots up, and the GGSN processor tries to sync the PDP contexts as standby, exception happens a couple of times before the GGSN coming up finally. The problem doesn't always happen consistently, though.

Workaround: There is no workaround.

- CSCsh48919

Symptoms: A "dir disk0:" command will fail if any filename or directory name stored on disk0 contains embedded spaces. This applies to disk1 or disk2 as well.

Conditions: A removable ATA flash card can be removed from the router and inserted into a laptop that is running a version of the Windows operating system. Then a "New Folder" directory can be created on the ATA flash card. The flash card can be removed from the laptop and re-inserted into the router. Typing the "dir" command on the router may fail to show all the stored files or in some cases crash the router.

Workaround: Remove or rename all files and directories having names with embedded spaces so that no file or directory names contains embedded spaces.

- CSCsh57509

Symptoms: A Cisco router that is configured for RIPv2 may not delete a path from the routing table when it should do so.

Conditions: This symptom is observed after the router has learned multiple paths for a prefix with different next hops from one neighboring router and after the neighboring router stops advertising one of the paths.

Workaround: Enter the **clear ip route *** command.

- CSCsh66935

Symptoms: Router Crashes in `avl_get_next_threaded`

Conditions: This symptom has been observed when deleting many tunnels with tunnel protection enabled. Happens in extremely rare cases.

Workaround: There is no workaround.

- CSCsh70638

Symptoms: When a router boots and when bursty traffic occurs, the following error messages may be generated:

```
%ALIGN-SP-STDBY-3-SPURIOUS: Spurious memory access made at 0x72AB2370 reading 0xB8
%ALIGN-SP-STDBY-3-TRACE_SO:
-Traceback= (s72033-adventerprise9_wan_dbg-0-dso-bn.so+0x1AE370) ([42:0]+0x1AE47C)
([31:-3]3-dso-b+0x220994) ([41:0]+0x220FB8) ([41:0]+0x221A90) ([41:0]+0x22214C)
([41:0] +0x222D6C) ([41:0]+0x2233CC)
```

Conditions: This symptom is observed when bursty IPC traffic occurs while the router boots or during a switchover, typically with heavy configuration data exchanges.

Workaround: There is no workaround.

- CSCsh71993

Symptoms: SIP may not pass the correct calling number in the header when an e164 address is used. SIP should block the population of the calling party number if the user portion of the "From" header is not an e164 address, preventing the calling party number IE from being populated when ISDN sends the SETUP message. However, this does not occur, and SIP may pass an incorrect number.

Conditions: This symptom is observed on a Cisco gateway that sends Microsoft Communicator SIP calls to the PSTN.

Workaround: There is no workaround.

- CSCsh72664

Symptoms: With a DMVPN setup running OSPF, OSPF neighbourship flaps and tracebacks are seen.

```
*Feb 9 12:20:34.147: %SYS-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from
0x605270B0, alignment 32
Pool: I/O Free: 396512 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

Conditions: With an mGRE tunnel with tunnel protection configured and OSPF running, the problem can occur if there is a route for a tunnel transport destination address for a spoke through the tunnel itself.

Workaround: The problem was seen with a DMVPN setup that was misconfigured so that a tunnel transport destination address was through the tunnel. The problem will be avoided if there are no routes for tunnel destination addresses through the tunnel.

- CSCsh75827

Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the "J" Service-Info attribute), has logged out from the SESM, and then renews its IP address.

Workaround: There is no workaround.

- CSCsh76895

Symptoms: Multiple conflicting conform / exceed /violate actions are allowed under a single classmap.

Conditions: The user is allowed to configure multiple conflicting conform/exceed/violate actions under the same class-map.

Workaround: There is no workaround.
- CSCsh85531

Symptoms: Some E1 channels may remain down after you have reloaded a router.

Conditions: This symptom is observed on a Cisco 7200 series that function as a PE router and that connects to a CE router. Both routers are connected through 1-port multichannel STM-1 (PA-MC-STM-1) port adapters and the **framing no-crc4** command is enabled on all interfaces of both routers.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of the PA-MC-STM-1 at the PE side to enable all interfaces to come up.
- CSCsh86888

Symptoms: When the **fax protocol t38 ls-redundancy value hs-redundancy value** command is enabled with values other than zero, redundant packets should be generated for MGCP T.38 fax calls, but this does not occur.

Conditions: This symptom is observed on a Cisco platform such as a Cisco AS5400 that runs Cisco IOS Release 12.4 or interim Release IOS 12.4(11.5)T.

Workaround: There is no workaround.
- CSCsh88792

Symptoms: A router that is configured for Dynamic DNS (DDNS) may reload unexpectedly.

Conditions: This symptom is observed when you manually change the IP address of an interface that has DDNS configured.

Workaround: There is no workaround.
- CSCsh91974

Symptoms: RP crash.

Conditions: Some of the PIM CLIs are causing active RP to crash. This is happening ONLY when these CLIs are configured while in the sub-config mode for "control-plane policing". Normally, any global relevant config should automatically exit the sub-config prompt, and accept the CLI as well. In this case, the PIM command is rejected and RP crash follows. The same PIM commands work fine when executed under the global config mode (where they belong) or under other sub-config modes.

Workaround: Use the "exit" command to exit the the main config prompt before configuring PIM related CLIs.
- CSCsh98300

Symptoms: A router performing traceroute may crash if name lookup is enabled.

Conditions: This symptom has been observed when running Cisco IOS images which have the fix for CSCuk25309 or CSCuk33415.

Workaround: Disable name lookup using the **no ip domain-lookup** global configuration mode command when doing traceroute.

- CSCsi10945

Symptoms: After a user is prompted to enter their user name and password, a token response field is displayed without the actual token or SNK challenge. The output of the **debug radius** command shows that the SNK challenge is sent to the user, but it is not displayed on screen.

Conditions: This symptom is observed on a Cisco router when the **ip auth-proxy** command is configured for HTTP with a one-time password (OTP).

Workaround: There is no workaround.

- CSCsi11996

Symptoms: The following error message is displayed on a Cisco AS5850 router every hour:

```
%HA_CLIENT-3-NO_CF_BUFFER: The MARVEL CRYPTO HA client failed to get a buffer
(len=1120) from CF (rc=1); checkpointing failed
-Traceback= 0x201C9FBC 0x217C1B58 0x217C2068 0x21BBD32C 0x21BBDFD0 0x21BBE180
0x21DCF368 0x21DCF5C4
```

Conditions: This symptom has been observed on a Cisco AS5850 gateway running crypto images (c5850tb-k9p9-mz) in RPR+ mode.

Workaround: There is no workaround.

- CSCsi20225

Symptoms: Continuous tracebacks may be generated on an LNS.

Conditions: This symptom is observed when you bring up PPPoX or L2TP sessions over multiple tunnels without traffic being processed over these sessions.

Workaround: There is no workaround.

- CSCsi24939

Symptoms: A router may reload unexpectedly when using a CA that does not support the GetCAPS exchange (part of SCEP), because of a bus error crash after entering the **crypto ca authenticate** command.

Any response other than a real GetCAPS reply will cause the crash. Before the router crashes, the following error messages and traceback are generated:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Crypto CA.
-Traceback= 0x42AB7410 0x424A6E18 0x42469B7C 0x424651E0 %Software-forced reload
Preparing to dump core... %CRYPTO-4-IKMP_NO_SA: IKE message from xxx.xx.xx.x has no SA
and is not an initialization offer
```

Conditions: This symptom is observed on a Cisco 2821 that runs Cisco IOS Release 12.4(10b) but may not be platform-specific.

Workaround: There is no workaround.

- CSCsi27540

Symptoms: A VSI session may become stuck in the "RESYNC_UNDERWAY" state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

Workaround: There is no workaround.

- CSCsi43340

Symptoms: DSMP is not programming the DSP for supervisory tone while alerting tone is there, which leads to the fxo disconnect supervision issue.

Conditions: This symptom has been observed when using a Cisco IOS software version later than Cisco IOS Release 12.3(14)T.

Workaround: Change to Cisco IOS Release 12.3(11)T.

- CSCsi51682

Symptoms: The **microcode reload pxf** command does not function.

Conditions: This symptom is observed on a Cisco RPM-XF that runs Cisco IOS Release 12.4 or Release 12.4T and occurs either with the **microcode reload pxf** command or the **microcode reload sar** command. However, the symptom is not platform-specific.

Workaround: There is no workaround.

- CSCsi54186

Symptoms: A Cisco IAD 2400 series may reject sequence numbers for Q.921, causing calls to be dropped or a PBX to lock up.

Conditions: This symptom is observed when a Cisco IAD 2400 series is connected to a third-party vendor phone system and third-party vendor PBX and occurs only when sequence number 16 or 68 is sent to the IAD.

Workaround: There is no workaround.

- CSCsi54519

Symptoms: The first time a Cisco IOS IPS 4.x signature performs an inline deny action against a flow and/or attacker, a dynamic ACL is created. However, subsequent times a deny action is performed, the signature does trigger but no dynamic ACL is created.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(9)T3 with advanced IP services when Cisco IOS IPS has a signature action that is configured for "denyinlineflow" and/or "denyattackerinline" and when Cisco IOS IPS is enabled on an interface in the outbound direction.

Workaround: Enable Cisco IOS IPS on an interface in the inbound direction only.

- CSCsi55964

Symptoms: After a gateway receives a high number of calls, calls may not go through intermittently.

Conditions: This symptom is observed on a Cisco 3800 series that functions as a gateway and that is configured for E1R2 signaling. The symptom occurs when the gateway sends a "clear forward" forward to the PSTN before the PSTN sends a "B1" message.

Workaround: There is no workaround.

- CSCsi57197

Symptoms: The T.37 Fax Offramp process may leak small amounts of memory.

Conditions: This symptom is observed on a Cisco router when the fax call on the PSTN side hangs up before the call completion.

Workaround: There is no workaround.

- CSCsi59685

Symptoms: One-way audio may occur and DTMF digits may not function.

Conditions: This symptom is observed on a Cisco gateway such as a Cisco AS5400 after a SIP transfer has occurred.

Workaround: Enter the **no voice-fastpath disable** command to resolve the one-way audio issue. There is no workaround for the DTMF issue.

- CSCsi60004

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

- CSCsi62152

Symptoms: A Cisco router that is configured for IPsec HA may generate a "SYS-2-CHUNKMALLOCFAIL" error message and a traceback.

Conditions: This symptom is observed on a Cisco 3845 that functions as an EzVPN server. The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCsi64450

Symptoms: Many time out errors and many retries without any other IPC errors will be seen.

Conditions: This symptom is observed on a Cisco AS5850 platform.

Workaround: There is no workaround.

- CSCsi67763

The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

<http://www.kb.cert.org/vuls/id/739224>

By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml>

- CSCsi70791

Symptoms: A Cisco router can experience a memory corruption crash related to encryption.

Conditions: This symptom has been observed when the **memory lite** global configuration command is disabled.

Workaround: Enable the memory allocation lite (malloc_lite) feature by using the **memory lite** command.

- CSCsi70920

Symptoms: In a scenario where traffic is passed to and from two different interfaces, both with the **ip admission** command configured, EAP over UDP communication will only be triggered for hosts initiating traffic.

This situation results in return traffic that should be allowed after completing the NAC process (for example, via NAC exemption) to be blocked.

Conditions: This symptom has been observed when the **ip admission** command is configured on two communicating interfaces and NAC needs to be triggered in order to open traffic for return traffic.

Workaround: Instead of sending traffic from A->B and B->A, trigger traffic from A->B and if B sends traffic to any other dummy destination like C. This results in NAC to be triggered for A when it sends the traffic to B, and B will be posture validated when it sends traffic to C.

- CSCsi72121

Symptoms: Calls via IPIPGW bow working. Calls from CCM over H323 to CME using GK controlled trunk via IPIP GW

Conditions: This symptom has been observed with 12.4(13.13)T2 IOS image .

Workaround: Use previous version of Cisco IOS software on IPIP GW

- CSCsi76936

Symptoms: Router may crash when "debug glbp" is enabled.

Conditions: Only occurs when GLBP receives a packet from a group that is not configured locally.

Workaround: Do not enable GLBP debug.

- CSCsi81801

Symptoms: The **h245 caps suppress nte** command may not function, causing an IPIPGW to continue to advertise the NTE capability in an H.245 capability message.

Conditions: This symptom is observed on a Cisco router that functions as an IPIPGW and that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: There is no workaround.

- CSCsi82336

Symptoms: Plugging a V.35 DTE cable into an HWIC-4T Serial port in "shutdown" state may result in the "shutdown" command being removed and the interface coming up/up.

The issue is observed 3845/HWIC-4T/c3845-advsecurityk9-mz.124-13b

Conditions: This symptom has been observed with 3845/HWIC-4T/c3845-advsecurityk9-mz.124-13b.

Workaround: Manually re-add "shutdown" command to serial interface.

- CSCsi83724

Symptoms: Ping between CE routers failed, after flapping PE routers interface or flapping ip cef on PE routers.

Conditions: This symptom has been observed with ATM PVC adjacency between PE and CE becomes incomplete when interface or ip cef is flapped on PE routers.

Workaround: There is no workaround.

- CSCsi84017

Symptoms: When you reload a Cisco 2600 series, the router may hang.

Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsi84591

Symptoms: When an SSG does not receive a RADIUS accounting stop message for a particular user from an Access Zone Router (AZR), the same user (with the same MAC address) does receive a new IP address from the AZR (which is also a DHCP server). In this situation, SSG receives the accounting start message from the AZR and does acknowledge the receipt, but may not create any input in the RADIUS proxy user table.

Conditions: This symptom is observed when the hotspot is part of a network that is configured as an SSG RADIUS proxy client.

Workaround: There is no workaround.

- CSCsi84605

Symptoms: show IMA interface IMA X/Y display wrong timing reference link after changing the clock source.

Conditions: After changing the network clock priority to be source clock, IMA still shows the previous clock source. Also tried to shut and not shut on the previous interface.

Workaround: There is no workaround.

- CSCsi84767

Symptoms: T38 fax outbound to the Cisco AS5850 gateway fails.

Conditions: After upgrading from Cisco IOS Release 12.3(11)T9 to Release 12.4(7e), it is observed that fax calls from an analog Cisco 2420 or Cisco 2430 router outbound to the Cisco AS5850 fail. It appears the Cisco AS5850 is having trouble falling back from T38 to passthrough. Standard configuration is T38 enabled on the Cisco AS5850 but not on the analog IAD. Disabling T38 on the Cisco AS5850 results in successful faxing.

Workaround: There is no workaround.

- CSCsi85641

Symptoms: When the Reverse Route Remote Peer option is enabled, packets may not be forwarded correctly.

Conditions: This symptom is observed when both CEF and the **reverse-route remote-peer** command are enabled. When you enable the **debug ip cef drops** command, typically, the following is shown:

CEF-Drop: Stalled adjacency for remote-physical-ip-addr on Ethernet1/0 for destination remote-protected-ip-addr CEF-Drop: Packet for remote-protected-ip-addr -- encapsulation

Workaround: Disable CEF.

Alternate Workaround: Add a next hop to the reverse route, for example, by entering the **reverse-route remote-peer ip-address** command.

- CSCsi93066

Symptoms: An MGCP endpoint may become stuck and generate the following error message:

400 Nas Software error

Conditions: This symptom is observed when a call agent sends a CRCX message after a modem reset.

Workaround: Shut/no shut on the controller.

- CSCsi97434

Symptoms: The router will crash when ipsec is established only in the case when both PKI and IKE AAA accounting is configured. When PKI is configured, the DN is used as the isakmp identity. The crash only occurs when the DN is not available and the server tries to use the DN as the isakmp identity.

Conditions: This symptom has been observed with a router running 12.4(13b) acting as a dmvpn hub may crash when you clear the isakmp peer and the session is reestablished. The certificate for the crypto peer is from a PKI server

Workaround: There is no workaround.

- CSCsi99217

Symptoms: When 6000 L2TP sessions are disconnected, a Cisco IOS LNS router is stuck on High CPU Utilization (99% or 100%) with PPP IP Route process for 5 minutes.

Conditions: This symptom has been observed under stress test conditions (thousands sessions are disconnected at once) with no traffic and using Cisco IOS Release 12.4(13). This symptom has not been observed on earlier releases.

Workaround: There is no workaround.

- CSCsj01861

Symptoms: Upon reload of Cisco 3825, acting as IPIPGW, SIP processing fails. Outbound SIP messages (requests or responses) fail to be sent.

Conditions: This symptom has been observed with a reload of IOS IPIPGW running 12.4(11)XW in the following topology:

IP phones --Callmanager---H323---IPIPGW---SIP---SBC-->PSTN

SIP bind commands are configured on the IPIPGW under 'voice service voip'

Workaround: To restore call functionality, remove the SIP bind statements in the configuration and add them back in.

Further Details Not observed when no SIP bind commands are configured.

- CSCsj04563

Symptoms: SSG memory is leaking in Cisco IOS Release 12.4(13b).

Conditions: This symptom occurs when the RADIUS proxy feature is used. Leaking could be triggered on the following call flow scenario:

1. HostObject(HO) with MSID1, ip-address IP1 and username user1@cisco.com is logged on.
2. PDSN sends an acct-stop with MSID1 with session-continue attribute set to TRUE. When this is received, SSG will start a hand-off timer. Note that SSG will not delete the HO at this time.
3. Hand-off timer expires. HO is deleted.
4. SSG now receives an acct-start with MSID1 and username user1@cisco.com.
5.
 - a. SSG will treat this as an auto-domain user, even though auto-domain is not configured on SSG.
 - b. SSG will try to get the profile by extracting the domain name from the structured username and sending an access-req to AAA with username as the domain name.
 - c. Since AAA server does not have the cisco.com profile, it sends an access-reject to SSG.
6. No HostObject is created.

Workaround: There is no workaround.

- CSCsj06177

Symptoms: RPR+ mode, when I do the following sequence the slave RSP configs add a "shutdown" command under interface serial.

Conditions: This symptom has been observed with RSP runnig RPR+.

Workaround: Doing the follow steps:

```
interface serial x/x
shut
no shut
```

- CSCsj08606

Symptoms: A VWIC2-2MFT-T1/E1 may stay in alarm state after either shut/ no shutting the controller or removing and replacing the interface cable.

Conditions: This symptom has been observed when the controller is configured this way:

```
! controller E1 0/0/0 framing NO-CRC4 ds0-group 0 timeslots 16 type ext-sig ... ds0-group 30
timeslots 30 type ext-sig alarm-trigger blue 0 !
```

The problem has been observed in c3845-sp servicesk9-mz.124-9.T3

Workaround: Shut down and restart the controller or remove and replace the cable a second time.

- CSCsj13444

Symptoms: The "set ip next-hop" command misses some part of the next-hop addresses.

Conditions: whenever the input string crosses more than 255 characters for the command "set ip next-hop", the extra characters are truncated which means losing of some IP addresses.

This in turns affects the overall functionality of PBR.

Workaround: Configure the ipaddresses individually using seperate "set ip next-hop" command if the number of characters inputted crosses morethan 255 (i.e, you can't configure more than 255 characters via a single CLI).

- CSCsj23556

Symptoms: The fix of CSCsc63752 in hawaii caused the following boot images build failure, c4gwy-cboot-mz, c5850-boot-mz, and c7200-boot-mz.

Conditions:

Workaround: There is no workaround.

Further Problem Description: This issue is pretty understandable as deals with build breakage of boot images. The other than pointed images are built successfully.

The fix of CSCsc63752 is having a function call which is not defined in same sub-system from where we are calling that.

- CSCsj25395

Symptoms: Having a configuration similiar to this:

```
interface Dialer1 ip address <ip add> <mask> encapsulation
frame-relay dialer pool 1
dialer remote-name <other_end>
dialer string 0
dialer string oe_tn
```

```

dialer caller oe_tn
dialer max-call 1 dialer-group 1
frame-relay map ip <addr> <oe_dlcI> broadcast
frame-relay interface-dlcI <loc_dlcI>
frame-relay ip tcp header-compression
no shutdown ! And entering in the following will crash the device.
interface Dialer1
shutdown
no interface Dialer1

```

Conditions: Removing the Dialer interface configuration whilst having IPHC configured on that interface will crash the platform this is observed on Cisco7200 running "IS" 124(16.5).

Workaround: Remove any IPHC CLI from the Dialer interface prior to deleting the Dialer interface from the configuration.

- CSCsj27294

Symptoms: Abnormal delay in CRCX processing

Conditions: When the authentication is done before allocating the resources for the call.

Workaround: There is no workaround.

Further Problem Description: MGCP receives a CRCX and while processing it, it tries to allocate the necessary resources by calling the RM. Normally the resource allocation would take 40 to 50 ms and the RM would get back with SUCCESS/FAILURE. But in the failed case, even after 2 seconds, we don't see any response from the RM.

- CSCsj36088

Symptoms: **test ip domain lookup aaa.global.com non-block** command does not resolve the name

Conditions: This happens with non-block options with ip domain lookup for server name

Workaround: There is no workaround.

- CSCsj36237

Symptoms: The Client Router crashes, while shutting down the Interface, after it got an Ip Address from the DHCP server.

Conditions: This failure is seen in Cisco IOS Release 12.4(16.5)T.

Workaround: There is no workaround.

- CSCsj38088

Symptoms: Router is getting crashed while enabling ipv6 and ospf on the interface .

Conditions: This issue is seen for the Cisco IOS Release 12.4(16.9).

Workaround: There is no workaround.

- CSCsj43575

Symptoms: ACL entries were not NVGened correctly

Conditions: Problem seen in Cisco IOS Release 12.4(16.9) only.

Workaround: There is no workaround.

- CSCsj49349

Symptoms: A Cisco Route Switch Processor can unexpectedly reload and experience a switchover when a Versatile Interface Processor in the same router containing an ATM Port Adapter fails.

Workaround: There is no workaround.

- CSCsj50773

Symptoms: Performing an snmpwalk on the ipRouteTable MIB may cause high cpu and reloads.

Conditions: Router has Cisco IOS Release 12.4(13b) or later.

Workaround: Create a view that excludes the ipRouteTable:

```
snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude
snmp-server view cutdown internet included
snmp-server community <comm> view cutdown RO
```

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

- CSCsj58898

Symptoms: The problem is that the PCMM policy server polls the ifStackTable (1.3.6.1.2.1.31.1.2) on CMTSs to identify bundle interfaces.

in some cases, the following mibs contain wrong/missing informations:

ifStackHigherLayer (1.3.6.1.2.1.31.1.2.1.1)

ifStackLowerLayer (1.3.6.1.2.1.31.1.2.1.2) :

Conditions:

Workaround: There is no workaround.

- CSCsj63916

Symptoms: All DATA analog dialout call are setting Bearer Capability to 0x8090 instead of 0x0890A3 (indicating the x-Law) ..A3 being for A-law

Conditions: Cisco AS5xxx running image above Cisco IOS Release 12.4(7e) and having to make outgoing DATA calls.

Workaround: There is no workaround.

- CSCuk61910

Symptoms: PE router crashes while configuring MVPN.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsh36203

Symptoms: A Cisco router is crashing at p_dequeue.

Conditions: This symptom is observed when testing the Echo cancelling feature in the Cisco 1700 platform but is not platform dependent.

Workaround: There is no workaround.

- CSCsi91665

Symptoms: H.323 calls intermittently disconnect.

For each new call the H.323 GW will generate a TCP Port to be used for call setup. Intermittently the GW will generate a TCP Port that is being used for an established connection. When the GW initiates the three way handshake for the new call it receives a response with an unexpected ACK sequence number. The GW will then send a TCP RST causing the currently established TCP connection/call to be torn down.

Conditions: This symptom has been observed with both Cisco IOS Release 12.4(13a) and 12.4(13b).

Workaround: There is no workaround.

- CSCsj62846

Symptoms: A MIB walk of the udpTable will have extra bad entries when a UDP IPv6 connection to the box is made

Conditions: IPv6 must be configured, an IPv6 udp socket must be present

Workaround: There is no workaround.

Wide-Area Networking

- CSCek41543

A Cisco 2811 router running Cisco IOS Release 12.4(7a) may have a memory leak in the "ISDN" process as seen in show process memory. The leak rate appears to be about 1.20MB/Hour.

Conditions: This symptom has been observed with BRI-U interface that is UP/UP (spoofing).

Workaround: Administratively shut down the BRI interface.

- CSCek56693

Symptoms: ALIGN-3-SPURIOUS message seen on console.

Conditions: This symptom has been observed when ATM PVC is deactivated and the PVC is carrying PPPoA sessions.

Workaround: Deactivate the PPPoA sessions before deactivating the PVC.

- CSCsg89222

Symptoms: A PPP session that is initiated from a client may not be forwarded. to an LNS.

Conditions: This symptom is observed on a Cisco router after the PPP session has been established.

Workaround: Enter the **vpdn source-ip** global configuration command.

- CSCsh72559

Symptoms: sh pppoe throttled mac command may display no or Invalid output.

Conditions: This symptom has been observed when "sh pppoe throttled mac" command is issued

Workaround: There is no workaround.

- CSCsi28543

Symptoms: After reload, one of two dialer interfaces binds all bri's channels, and finally the dialer uses only one channel. However, the rest one channel not used remains to be bound to the dialer. Therefore, the other dialers can't use an idle channel. When the problem is occurred, idle bri channel's intf status will become "hardware:down line:up".

Conditions: This symptom has been observed when a router is rebooting, and its peer router over isdn begin to transmit packets.

Workaround: There is no workaround.

- CSCsi51507

Symptoms: A router may crash when a voice call is received.

Conditions: This symptom is observed on a Cisco router that has the **isdn overlap-receiving** command enabled.

Workaround: There is no workaround.

- CSCsi68761

Symptoms: Dialer interface with vrf checks the route in other vrf. This causes dialer interface no to go down by idle-timeout when the target route of dialer watch on other vrf doesn't exist in routing-table.

Conditions:

- VRF is configured on dialer interface.
- When the other vrf route on the other dialer profile is down
- When the dialer interface goes up by doing "ping".

Workaround: There is no workaround.

- CSCsi69009

Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase "cloned from: AAA, AAA, ..." (that is, multiple instances of AAA) as identification.

Workaround: There is no workaround.

Further Problem Description: You can alleviate the situation somewhat by configuring the NCP Timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

- Increase the hello timers for L2TP and for the receive windows.
- Configure the timers under the virtual template.
- Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
- Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

- CSCsi74960

Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

Workaround: There is no workaround.

- CSCsi83952

Symptoms: show isdn service shows b_channels of interface configured for primary ss7-nfas as outofservice

Conditions: This symptom has been observed with a Cisco AS5850 or Cisco AS5400 platforms for controller configured for ss7-nfas

Workaround: There is no workaround.

- CSCsi89048

Symptoms: A call may be present on a backup D-channel but the Call Control Block (CCB) information may be missing.

Conditions: This symptom is observed on a Cisco platform after you have entered the **isdn test l2 disconnect** command on the interface for a backup D-channel.

Workaround: There is no workaround.

- CSCsi95921

Symptoms: When dial-peer "stat" changes to down no calls can be made

Conditions: This symptom has been observed intermittently and does not seem to be related to any of the ISDN interface states

Workaround: There is no workaround.

- CSCsi98140

Symptoms: After reloading router with a serial WIC-1DSU-T1-V2 and Cisco IOS Release 12.4(9)T1 or 12.4(11)T1 and if the serial is configured for SLARP, then the interface will show in the Admin Down state after the router reloads. Occurs even when it is verified that the 'shutdown' command is not present in startup-config or the running-config files.

Conditions: This symptom has been observed with a Cisco 2800, WIC-1DSU-T1-V2 running SLARP. In codes: c2800nm-advipservicesk9-mz.124-11.T1 c2800nm-advipservicesk9-mz.124-9.T

Workaround: After router recovers from re-booting issue the 'no shut' command under the interface.

Further Problem Description: Issue not seen in VWIC-2MFT-T1. Was not able to recreate the issue in c2800nm-ipbase-mz.124-3e

- CSCsj10593

Symptoms: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(15.6) and that functions as a TGW with all PRI switch types from the user to the network side. The symptom occurs when the **isdn test call interface interface-number dialing-string** command is entered at the platform on which the call is initiated, when the originating gateway (OGW) is configured for the National ISDN (primary-ni) switch type, and when the TGW is configured for the NT DMS-100 (primary-dms100) switch type. The symptom may also affect Release 12.4T.

Workaround: There is no workaround.

- CSCsj30647

Symptoms: Configure OGW and TGW with "isdn global-disconnect for switch type basic-net3 To verify AOC for DISCONNECT message pass across from one end to another end. The voice is made from the call-starter which causes the TGW to crash.

Conditions: This symptom has been observed with Cisco IOS Release 12.4(16.5)T. This happens for switch type basic-net3.

Workaround: There is no workaround.

- CSCsj45426
Symptoms: Cisco AS5850 FBs crash.
Conditions: This symptom has been observed on entering the **no pri-group timeslots** command.
Workaround: There is no workaround.
- CSCsj68052
Symptoms: Platform will crash if enter either **no frame-relay ip rtp header-compression** or **no frame-relay map ip <ipadd> <dlci>**
Conditions: This symptom has been observed with any platform running any 12.4 Mainline release. For the purpose of the note this is apparent in latest Cisco IOS Release 12.4(16.6) on 7200 IS build, but have also recreated this on a Cisco 3845, and was reported by TAC on a Cisco 2800.
The problem occurs when there is more than one IP map configured for the same DLCI and IP header compression is configured.
Workaround: Do not configure more than one IP map on the same DLCI at the same time as IP header compression.
- CSCsj76378
Symptoms: Router crashes when configure a vc-group using a MFR bundle link interface.
Conditions: This symptom has been observed when attempting an invalid FRF.5 configuration.
Workaround: This is an invalid configuration. Use the MFR bundle interface instead of the bundle link.

Resolved Caveats—Cisco IOS Release 12.4(16b)

Cisco IOS Release 12.4(16b) is a rebuild release for Cisco IOS Release 12.4(16). The caveats in this section are resolved in Cisco IOS Release 12.4(16b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsk70446
Cisco IOS emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.
A traceback appears after the error message. This traceback is encountered with long URLs.
It is important to note that this error message does not imply that packet data is corrupted. However, it does provide an early indicator of other conditions that can eventually lead to poor system performance or a Cisco IOS restart.
- CSCse12395
Symptoms: Router does not fail over to the secondary TACACS+ server.
Conditions: Occurs while using third-party TACACS+ server. Authentication and authorization works as expected, but the TACACS+ server sends incorrect accounting response. The router errors on check keys failure for accounting response, but still does not failover to the second TACACS+ server in the list.
Workaround: There is no workaround.

Interfaces and Bridging

- CSCsk48455

Symptoms: ATM map is not created dynamically for multipoint sub-interface. Inverse Address Resolution Protocol (InARP) request and response are not processed by the router.

Conditions: This occurs when ATM point-to-point sub-interfaces are created, and then the sub-interfaces are unconfigured. New multi-point sub-interfaces are created with the same configuration as point-to-point sub-interfaces.

Workaround: There is no workaround.

- CSCsd66215

Symptoms: The **Show bridge** command on R0 reveals that the received MAC address of the DSL client is not in the bridge table (although the bridge table is populated fine on switch1). Subsequent traffic is broadcast to every PVC until any packet other than an ARP reply is received from the MAC address in question.

Conditions: Occurred on a Cisco 7200 router (R0) running Cisco IOS Release 12.2(31). The router is configured to bridge RFC1483 bridged traffic between ATM and fastethernet sub-interfaces. ATM sub-interfaces (each in a bridge group) have PVCs that connect to many DSL customers. The Fastethernet subinterface of R0 is connected to another router (R3) via a switch. R3 is performing routing for this bridge group using a BVI. When R3 sends ARP request for a DSL customer IP address, the ARP is bridged to an ATM subinterface and then broadcast to every ATM PVC. When the ARP reply is received on R0, it is bridged by R0 just fine and reaches routing interface on R3. The ARP table is populated on RE. Packets other than the ARP reply do populate bridge table on R0.

Workaround: There is no workaround.

IP Routing Protocols

- CSCsk28282

Symptoms: Fragment packets are not translated by NAT router.

Conditions: This problem occurs when the NAT rule has route-map that points to an ACL, and the ACL has a "domain" keyword, as follows:

```
ip nat inside source static 192.168.2.1 192.168.1.10 route-map TEST ! ip access-list
extended TEST deny udp any eq domain any permit ip any any
```

If the packet is not a fragment packet, this problem never occurs. The second fragment packet is affected but additional fragment packets are not affected.

Workaround: There is no workaround.

- CSCsk35985

Symptoms: The system crashes when the **show ipv6 ospf lsdb- radix** hidden command is entered.

Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

- CSCsk89546

Symptoms: OSPF routes are not populated in the Routing Information Base (RIB) with the next hop as traffic engineering (TE) tunnels.

Conditions: Occurs when multiple TE tunnels are configured and the tunnels come up or are shut/no shut simultaneously.

Workaround: **Shut/no shut** tunnels one at a time.

- CSCsh34417

Symptoms: Incorrect routing occurs due to bad BGP distance value.

Conditions: Occurs following the failover to a path with higher distance. When the original path is restored, the distance value is not updated.

Workaround: Clear the BGP route, which causes the correct distance value to be learned.

- CSCsh80008

Symptoms: Changes to a neighbor's weight do not take effect when followed by the **clear ip bgp x.x.x.x soft in** command.

Conditions: When a soft reconfiguration inbound is enabled along with the neighbor weight assigned directly to a BGP neighbor, issuing the **clear ip bgp ip_address soft inbound** command resets the neighbor weight to 0 or has no effect.

Workaround: Set the neighbor weight value as part of an inbound policy such as a route map.

Alternative workaround: If the neighbor command **soft reconfig-inbound** is removed, you can still refresh your routes from the peer. This will happen with route refresh (you will not see the difference). Relying on **soft reconfig-inbound** for refreshing the routes is discouraged.

- CSCsi58867

Symptoms: Using the **show ip route static** or **show ip route connected** commands causes excessive CPU usage and CPUHOG messages. Tracebacks are also observed.

Conditions: Occurred after 250,000 BGP prefixes were received from a single neighbor. This is common in a lab scenario, but less likely in a production network.

Workaround: Instead of the command above, use the **show ip route | i ^S** command.

- CSCsi76616

Symptoms: LDAP packet is modified while passing through NAT router causing LDAP to fail.

Conditions:

Network Topolgy

=====

LDAP server----->(fa00)NAT Router(fa01)----->LDAP client

The packet after the NAT router seems to have been fragmented and expanded to two parts in LDAP:

Case1 - LDAP failed without "no-payload"

=====

- case1_before_nat_router -----> NAT Router -----> case1_after_nat_router

- LDAP packet modified

Case2 - LDAP passed with "no-payload"

=====

- case2_before_nat_router -----> NAT Router -----> case2_after_nat_router

- LDAP packet unchanged

Workaround: There is no workaround.

- CSCsj09838

Symptoms: When the BGP session between a Route Reflector (RR) and PE router flaps, the RR may no longer send some routes to the PE router.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsi85222. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi85222>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **clear ip bgp * all in** command on the PE router to retrieve all routes from the RR.

- CSCsj22187

Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

Conditions: This problem may happen only if the BGP show command is started and suspended by auto- more before the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. Many BGP **show** commands may have this vulnerability, but in each case the problem only happens if the deconfiguration removes objects that are being utilized by the show command. Removing unrelated BGP configuration has no effect.

Workaround: Terminate any paused BGP show commands before beginning operations to remove BGP- related configuration. Pressing “q” to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

Miscellaneous

- CSCeg20335

Symptoms: A Cisco 10000 series may lose the PVC configurations for several subinterfaces and high CPU usage may occur. When you attempt to reconfigure the PVCs, error messages similar to the following may be generated:

```
Router#pvc 35/134 Unable to create PVC 35/134 on ATM1/0/0.10350134. Possibly multiple
users configuring IOS simultaneously Further info about other user: Process id: 42,
Process: Slot 1/0 CMD Process, TTY: 0, Location: Console Router(config-subif)#
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(7)XI1 or Release 12.2(27)SBB.

Workaround: Reload the router.

- CSCek71877

Symptoms: IPv6 pings are not working when the **atm route-bridged ipv6** command is configured on the UUT.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(13.5)T images.

Workaround: There is no workaround.

- CSCek75633

Symptoms: A router may crash when you attach a VC class to an ATM bundle.

Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

Workaround: There is no workaround.

- CSCsi81891

Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

Workaround: There is no workaround.

- CSCsi84767

Symptoms: A T38 fax outbound to the Cisco AS5850 fails.

Conditions: After upgrading from Cisco IOS Release 12.3(11)T9 to Cisco IOS Release 12.4(7e), it is observed that fax calls from an analog Cisco IAD2420 or Cisco IAD2430 outbound to the Cisco AS5850 fail. It appears the Cisco AS5850 is having trouble falling back from T38 to passthrough. Standard configuration is T38 enabled on the Cisco AS5850 but not on the analog IAD. Disabling T38 on the Cisco AS5850 results in successful faxing.

Workaround: There is no workaround.

- CSCsi90169

Symptoms: The following error message appears: "Copland ERROR->Slot(2):Cache is full, processed 5 out of 8."

Condition: This message is seen on a Cisco 3825 router with MGCP configuration and a NM-HDV.

Workaround: There is no workaround.

- CSCsj08606

Symptoms: A VWIC2-2MFT-T1/E1 may stay in alarm state after either shut/ no shutting the controller or removing and replacing the interface cable.

Conditions: The controller is configured as follows:

```
controller E1 0/0/0 framing NO-CRC4 ds0-group 0 timeslots 16 type ext-sig ... ds0-group 30
timeslots 30 type ext-sig alarm-trigger blue 0
```

The problem has been observed in the c3845-spservicesk9-mz.124-9.T3 image.

Workaround: Shut/no shut the controller or remove and replace the cable a second time.

- CSCsj08617

Symptoms: E1 interface that is used for providing TDM network clock sometimes gets stuck in SHUTDOWN state after a controller failure, even after the controller is up and functioning.

Conditions: Occurs when E1s are used for T-CCS to connect together two PBX circuits across a WAN. The problem is intermittent. Sometimes the TDM clock is able to recover, but other times the network clock state from the **show network-clocks** command shows SHUTDOWN for an E1 controller that is up and working. The following shows the output when this happens:

```
router#show network Network Clock Configuration ----- Priority
Clock Source Clock State Clock Type
1 E1 2/0/0 SHUTDOWN E1 2 E1 2/0/1 GOOD E1 3 E1 2/0 SHUTDOWN E1 4 E1 1/0 GOOD E1 5 E1
1/1 GOOD E1 11 Backplane GOOD PLL
Current Primary Clock Source ----- Priority Clock Source Clock
State Clock Type
2 E1 2/0/1 GOOD E1
E1 2/0/0 is up. Applique type is Channelized E1 - balanced Description: No alarms
detected. alarm-trigger is set to Blue Alarm is not triggered Version info Firmware:
20060711, FPGA: 13, spm_count = 0 Framing is NO-CRC4, Line Code is HDB3, Clock Source
is Line. Current port master clock:recovered from backplane Data in current interval
(792 seconds elapsed): 0 Line Code Violations, 0 Path Code Violations 0 Slip Secs, 0
Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins 0 Error Secs, 0 Bursty Err Secs, 0
Severely Err Secs, 0 Unavail Secs
```

Workaround: Remove then reapply the network-clock-select command for the TDM clock in SHUTDOWN state. Use the following commands:

```
config t
```

```
no network-clock-select X E1 x/y
```

```
network-clock-select X E1 x/y
```

- CSCsj12558

Symptoms: BRI and PRI become active, and communication is normal. After about three minutes pass, ping loss might intermittently be observed.

Conditions: CEF drop was observed in interface with legacy dialer configuration or dialer rotary-group configuration in an end-to-end communication when enabling “debug ip cef drops”. At this time, ping loss was observed, and it was displayed as “incomplete” in show adjacency. This symptom was observed when using 12.4(13) or later. However, this symptom was not observed for interface with dialer profile configuration in an end-to-end communication.

Workaround: Disable cef(no ip route-cache cef). Use a Cisco IOS release that is not affected. Use dialer profile configuration instead of legacy dialer configuration or dialer rotary-group configuration

- CSCsj17772

Symptoms: When terminating an inbound SIP VoIP call to an ISDN PRI or BRI trunk, if the INVITE has a Remote Party ID whose calling party number is preceded with a “+” character, this character is retained in the outgoing ISDN Q.931 SETUP message. This may cause problems for some PBXs that do not ignore this character and consider it a literal in the calling party number.

Conditions: Occurs on Cisco IOS Voice Gateways configured for SIP VoIP and with ISDN PRI or BRI trunks.

Workaround: Use Cisco IOS Release 12.3(12.3)T, 12.3(11)T07, which are unaffected by this issue. You can also configure a translation rule to strip the leading “+” character and apply it to the POTS dial-peers assigned with the PRI and BRI voice-ports.

- CSCsj21562

Symptoms: During bootup, “send break” does not erase NVRAM when “no service password-recovery” is configured. The router does not respond to the break sequence. When enabling recovery, the customer can break the router into ROMMON without any issues.

Conditions: Occurs on a Cisco 3845 router running Cisco IOS Release 12.4(13b).

Workaround: There is no workaround.

- CSCsj27183

Symptoms: H323-->SIP interworking fails for a Fast start call when transcoding is enabled on an IPIPGW. Transcoding is done between G711ulaw and G729r8 codecs.

Conditions: This failure is seen for H323--SIP--SIP--SIP and H323--SIP--SIP-- H323 call flows when transcoding is enabled on IPIPGW1. It is also seen on H323--H323--H323--SIP call flow for transcoding on IPIPGW2. This is seen only with a Fast Start call (both with H245 Tunnel enabled and disabled), and the call passes with a slow start call.

Workaround: There is no workaround.

- CSCsj37709

Symptoms: Memory held by mem_mgr_chunk_t and mem_mgr_mempool_t in dead process is causing an out-of-memory condition on the gateway.

Conditions: This scenario occurs when SIP phone calls are made using the default application or a TCL IVR application and the **header-passing** command is enabled in voice service VoIP SIP configuration mode.

The following processes are the cause of the large amount of holding memory in *Dead* process:

```
0x61EC066C mem_mgr: mem_mgr_chunk_t
0x61EC091C mem_mgr: mem_mgr_mempool_t
```

Workaround: Disable the **header-passing** command.

- CSCsj38342

Symptoms: An MGCP gateway may unregister from Cisco Unified CallManager (CCM) when its device pool is reset. The **show ccm-manager** command shows that the gateway is registered to CCM but the CCM administration page shows it in the “Unregistered” state.

Condition: This problem was observed when the gateway had a TFTP failure in downloading the XML configuration file.

Workaround: Enter the **no mgcp** and **mgcp** commands in router configuration mode to force the gateway to register.

- CSCsj40156

Symptoms: Memory is leaking in case of radius-proxy users.

Conditions: This symptom is seen when a rad-proxy host object is already present in the SSG box, and it receives the access-request. The accounting starts from the proxy client, which is sent to the AAA server and AAA replies with an access-accept.

Workaround: There is no workaround.

- CSCsj46178

Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router in either global MGCP configuration or MGCP profile.

Workaround: Do not configure the **endpoint naming t3** command. Use t1 endpoint naming instead.

- CSCsj49255

Symptoms: If there is an ACL and DSCP being used for packet matching on class-map, only the first packet descriptor will get a match, and everything else will not. If DSCP is removed, the packet matching works again.

Conditions: This symptom is observed on a Cisco 7200 with ACL and DSCP with match all option.

Workaround: There is no workaround.

- CSCsj50773

Symptoms: Performing the **snmpwalk** on the ipRouteTable MIB may cause high CPU and reloads.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

Workaround: Create a view that excludes the ipRouteTable:

```
snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude
snmp-server view cutdown internet included
snmp-server community <comm> view cutdown RO
```

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

- CSCsj53228

Symptoms: When there are call disconnects happening with the last controller of an STM interface on a Cisco AS5850, the box crashes with tracebacks. This occurred in a scenario where the Cisco AS5850 is acting as terminating gateway with STM card on slot 0. The last controller of the STM, 0/0.3/7/3 is configured for E1/R2. Full controller worth calls are being made. No other calls are up other than last controllers' 30 calls. The call stays for the specified call duration. Once the call starts disconnecting, the Cisco AS5850 crashes with traceback decode function pointing to "csm call disconnect".

Conditions: This issue is seen only when the calls are on the last controller. (63rd => 0/0.3/7/3). In a similar scenario tested with other controllers with similar configurations, the issue is not seen.

Workaround: There is no workaround.

- CSCsj58969

Symptoms: Executing the **show port modem calltracker** command on a Cisco AS5400XM can cause bus error crash.

Conditions: This symptom occurs on a Cisco AS5400XM with multiple calls being made and terminated when running Cisco IOS Release 12.4(13a).

Workaround: There is no workaround.

- CSCsj64230

Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

Workaround: There is no workaround.

- CSCsj67725

Symptoms: DTMF digits are not forwarded when a call is answered during the off phase of a ring cycle. Digits are forwarded only during the on phase.

Conditions: Occurs with the following POTS dial peer definition, which terminates a call to an analog FXS LoopStart voice-port:

```
dial-peer voice 4634099 pots
destination-pattern 463....
port 2/21
forward-digits all
prefix , , !
```

When a called number matches this dial peer, the DTMF digits should be forwarded two seconds after the connection is made. It has been discovered that this works as expected provided that the call is answered during the on phase of the ring cycle only, but that no digits are forwarded if the call is answered during the off phase.

This behavior has been observed on Cisco VG224 and Cisco IAD2430 voice routers with analog FXS voice ports and the FXS Analog Voice Module V2.1 installed. It occurs when running Cisco IOS releases that include the fix for bug ID CSCse92359.

Workaround: (1) Set **idle-voltage low** under the voice-port if it is an analog FXS port and the command is available.

(2) For current IOS 12.4 mainline and 12.4T releases, use the “ring cadence” command under voice-port configuration mode to define a custom ring cadence where the duration of the on phase of the ring cycle is large and the duration of the off phase is small in comparison, giving the called party the best chance to answer the call during the ON phase.

! voice-port 2/21 ring cadence define 50 1 /* 5000ms ON, 100ms OFF */ !

Notes:

(A) voice-port commands entered in workaround options (1) and (2) above should be followed with a **shutdown/no shutdown** to ensure that the new settings take effect.

(B) Workaround options (1) and (2) are mutually exclusive. Choose one option or the other.

- CSCsj72647

Symptoms: On a Cisco IOS voice gateway, the **show call active voice brief** command output on the IP leg shows rx counters stay at 0 for 46 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7e).

Workaround: There is no workaround.

- CSCsj74433

Symptoms: Cisco IOS throws “Undefined Error” when an empty file is being copied.

Conditions: Reproducible on most Cisco IOS releases.

Workaround: There is no workaround.

- CSCsj77659

Symptoms: Billing information relying upon AAA stop records from a Cisco IOS VoIP gateway may show different called number information after upgrading to a Cisco IOS 12.4 release.

Conditions: A Cisco IOS VoIP gateway configured with AAA accounting for VoIP call legs may display the Called-Station-Id for the Telephony call leg differently in Cisco IOS versions of 12.4 when compared to IOS versions prior to 12.3(14)T. This can occur when also running a TCL IVR script on the Cisco IOS gateway. In Cisco IOS Release 12.3, the Called-Station-Id would indicate the destination called number from the final VoIP call leg dialed. With Cisco IOS Release 12.4 versions, the Called-Station-Id indicates the original dialed number from the PSTN call leg.

Workaround: Modify the server receiving the AAA stop record to pull the Called-Station-Id from the VoIP call leg record.

- CSCsj87668

Symptoms: A Cisco AS5300 or Cisco AS5400 controlled by a Call Agent sends one packet with wrong RTP SSRC sequence number when changing from G.711 to GSM Codec

Conditions: Occurs only when changing from G.711 to GSM codec.

Workaround: Configure the **no voice-fastpath enable** command. This has a performance impact.

- CSCsj95947

Symptoms: The following message is seen on the router:

```
*Aug 6 16:34:47.188: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x8005EC50,
-Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50 0x800651E4 0x800652A8
0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0 0x809E42D4 0x80A0854C 0x800DB8C0
0x800DEE48
```

Conditions: The conditions under which this symptom occurs are not known at this time.

Workaround: There is no workaround.

- CSCsj96577

Symptoms: A Cisco AS5400HPX crashes due to a bus error as indicated by show version “System returned to ROM by bus error at PC 0x61728370, address 0xB0D0B45”.

Just before the crash the following error message is seen:

```
%SYS-2-NOTQ: unqueue didn't find 674D6D40 in queue 3C -Process= "MGCP Application",
ipl= 0, pid= 170
```

Conditions: This symptom is observed on a Cisco AS5400HPX.

Workaround: There is no workaround.

- CSCsj99478

Symptoms: Errors occur on a Cisco AS5850 Universal Gateway after online insertion and removal (OIR) of cards. Using the **debug snmp packets** command after OIR reports NO_SUCH_INSTANCE_EXCEPTION error for “cefcModuleOperStatus” and “cefcModuleStatusLastChangeTime”.

Conditions: Occurs on a Cisco AS5850 running image c5850tb-p9-mz.124-7c.bin and includes line “snmp-server enable traps fru-ctrl”

Workaround: There is no workaround.

- CSCsk02643

Symptoms: A Cisco router may reload with a software forced crash:

```
Jul 23 12:26:07.263: %FDM-3-TCAM_ENTRY_MISSING: FDM appl=3 test key=0x5A5A5A5A
internal key=0x5A5A5A5A5A5A5A5A missed a direct hit reading in TCAM after insertion.
Jul 23 12:26:08.399: %DM-6-ROOT_CAUSE_DETECTED: Component rsc-tcam-rw detected as a
root cause of a failure.
% Health Monitor reloading this RSC due to Zero system health
% Flushing last minute of Health Monitor events
Jul 23 12:26:08.503: %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a reload due
to Zero system health
%Software-forced reload
```

Conditions: Occurred on a Cisco AS5850 running Cisco IOS Release 12.4(13b).

Workaround: Disable the “rsc-tcam-rw diagnostic monitor” as follows:

```
RSC(config)#diagnostic-monitor
RSC(config-dm)#no test rsc-tcam-rw ?
active Disable on active only
standby Disable on standby only
RSC(config-dm)#no test rsc-tcam-rw active
Reset test result(s) to pass?? [yes/no]: yes
```

- CSCsk60020

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

- CSCsk73104

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

- CSCsb54207

Symptoms: MGCP Audit Endpoint (AUPE) response does not include “telephone-event” even though this capability is present.

Conditions: The “telephone-event” response was suppressed in order to prevent a conflict with Cisco Unified CallManager (CCM) versions 3.x/4.0. Later versions of CCM require the capability to be reported in order to enable it. The effect is that “telephone-event” functionality is not negotiated even though the gateway supports it.

Workaround: Use MGCP without “telephone-event”.

- CSCsc64217

Symptoms: Cisco router with “ip inspect sip” configured may crash after experiencing excessive CPU usage and eventual Watchdog Timeout in the “Inspect Timer” process.

Conditions: This bug is platform and software independent.

Workaround: Disable “ip inspect sip”.

- CSCse76935

Symptoms: A router that is configured for SNA Switching Services (SNASw) may crash.

Conditions: This symptom is observed when links with an end node go down and when there are multiple links to the end nodes, at least one of which supports CP-CP sessions, and one of which does not. The symptom occurs on rare occasions because of a timing condition.

Workaround: Change the end node device configuration such that all links to the SNASw router support CP-CP sessions. As per the APPN architecture, only one link does actually support CP-CP sessions.

Further Problem Description: The symptom occurs because there is a mix of APPN links (that support CP-CP sessions) and LEN links (that do not support CP-CP sessions) from an end node to the SNASw router. The recommended configuration is to have all links between two partners be of the same type. Because LEN links generally do not support parallel TGs, most likely these should be APPN links, all supporting CP-CP sessions. This is a product-dependent configuration on the end node product.

- CSCsg44008

Symptoms: Memory leak occurs on Cisco 3845 router.

Conditions: Occurs while making transfer call between SIP and SCCP.

Workaround: There is no workaround.

- CSCsg48190

Symptoms: A Cisco VoIP gateway with modem passthrough configured does not enable echo cancellation upon detection of 250 msec of silence.

Conditions: When using modem passthrough, the gateway disables the echo cancellation for that call upon detection of a ANSam modem tone. When a silence of 250msec in that call is detected, the echo cancellation should be enabled.

Workaround: This issue seems to occur in Cisco IOS Release 12.3(14)T and later. Switch to a Cisco IOS release that does not exhibit this symptom.

- CSCsg91306

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsh20656

Symptoms: TCP exchange with third-party clients frequently experience retransmissions from the client to the server.

Conditions: Occurs when TCP header compression is enabled. Clients using Microsoft dial-up networking (MS DUN) are not affected.

Workaround: Use a Cisco IOS Release 12.1, where the problem has not been detected. You can also disable TCP header compression and rely on Microsoft Point-to-Point Compression (MPPC).

- CSCsh22725

Symptoms: Outbound calls fail on a MGCP-controlled CAS channel on a Cisco VoIP gateway.

Conditions: This symptom is observed when the following conditions occur:

- A timeslot on an E&M T1 trunk is taken out of service from the connected switch side, showing as a permanent inbound seizure. In this situation, the output of the **show voice call summary** command indicates that the status for this channel is "EM_PARK".

- A Cisco CallManager that interworks with the Cisco VoIP gateway checks the status of the trunk via an MGCP AUEP command. The gateway responds with an "ES: rlc" message, which indicates that the trunk is available for calls.

Because the reported availability and actual availability of the channel are mismatched, all outbound calls on the channel fail.

Workaround: Attempt to clear the out-of-service state from the connected switch side. If this is not possible, when interworking with the Cisco CallManager, first enter the **shutdown** command followed by the **no shutdown** command on the voice port and then enter the same commands on the T1 controller. Doing so causes the gateway to send an NTFY message that indicates that there is an inbound seizure on the channel.

- CSCsh99624

Symptoms: Voice port is up, but the port monitored by busyout commands is still down. Occurs with the following configuration: voice-port xx/xx:xx cptone JP busyout action shutdown busyout monitor FastEthernetxx/xx

Conditions: Occurs on a Cisco 3745 router running Cisco IOS Release 12.3(14)T7 and Cisco IOS Release 12.4(12).

Workaround: There is no workaround.

- CSCsi11796

Symptoms: Trace back "CHUNKSIBLINGS: Attempted to destroy chunk with siblings" occurs.

Condition: Occurs on Cisco 2600 series routers running Cisco IOS Release 12.4(11)T2.

Workaround: There is no workaround.

- CSCsi20225

Symptoms: Continuous tracebacks may be generated on an LNS.

Conditions: This symptom is observed when you bring up PPPoX or L2TP sessions over multiple tunnels without traffic being processed over these sessions.

Workaround: There is no workaround.

- CSCsi28788

Symptoms: Traceback seen on Cisco AS5850 Universal Gateway while running stress calls.

Condition: Seen on Cisco AS5850 running Cisco IOS Release 12.4(13). “mgd_timer_stop” traceback is seen while running H.323/SS7 stress calls.

Workaround: There is no workaround.

- CSCsi29174

Symptoms: On a Cisco IOS voice gateway, the tx and rx counters in the output of the **show call active voice brief** command may not function properly. The counters may not increment at all or may increment in bursts every 10 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7c), Release 12.4(7d), Release 12.4(8c), or Release 12.4(13a).

Workaround: There is no workaround.

- CSCsi29843

Symptoms: The following issues related to BITS clock occur on Cisco ISR platforms: 1) Network clock is not switching to the next available reference when the receiving AIS on non-BITS port. 2) When unplugging the cable on BITS port, the network clock keeps switching back and forth between the BITS and the next available reference

Condition: These issues have been observed on Cisco IOS Release 12.4(13)T.

Workaround: Do not unplug the cables on BITS ports.

- CSCsi51838

Symptoms: Cisco ISR Routers using VWIC-MFT E1 cards (not VWIC2-MFT E1 cards) may experience some errors under traffic load.

Conditions: This problem appears to occur when unframed mode is configured on the controller.

Workaround: Run the E1 controller with a framed mode configured such as “channel-group 0 timeslots 1-31” instead of “channel-group 0 unframed”.

- CSCsi54519

Symptoms: The dynamic ACL which is applied once a signature is triggered (with denyAttackerInline and/or denyFlowInline Event Actions configured) never expires, and the same dynamic ACL may be displayed (each with different counter values) multiple times using the “show ip access-list dynamic” command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(9)T3 with advanced IP services when Cisco IOS IPS has a signature action that is configured for “denyinlineflow” and/or “denyattackerinline” and when Cisco IOS IPS is enabled on an interface in the outbound direction.

Workaround: Enable Cisco IOS IPS on an interface in the inbound direction only.

- CSCsi56491

Symptoms: Multiple VLAN with access lists causes reload.

Conditions: Three VLANs are configured on a gigabit interface on a Cisco AS5850 Universal Gateway. On each VLAN access-lists are applied. The configuration is tested after initial configuration and works as expected. However, if the Cisco AS5850 is reloaded, the behavior changes and the access lists are not working as before. This is seen by the change in the traffic going through the access list. It seems that VLANs and access lists get mixed or not correctly applied after the reload. There is no visual loss of configuration.

Workaround: Enter configuration mode for the affected sub-interface. Doing so immediately corrects problem.

- CSCsi74220

Symptoms: SSH version 2 sessions to a Cisco IOS device may not cleanly exit in a timely manner and may consume large amounts of CPU cycles until they are manually or automatically cleared.

Conditions: This occurs in Cisco IOS software versions 12.4(7.2) and 12.4(7.2)T and later. This behavior seemed to be eliminated in 12.4(9.9) and 12.4(9.9)T but then was reintroduced in 12.4(9.15) and 12.4(9.15)T with a slight change in behavior. In 12.4(9.15) and 12.4(9.15)T the behavior changed such that the sessions seem to clear themselves after about 3 minutes. This has only been seen with the SSH client that connects to the IOS device is the SSH client provided by CiscoWorks.

Workaround: Use SSH version 1.

- CSCsi77147

Symptoms: DTMF path confirmation is not received for a SIP call.

Conditions: This problem is due to an issue with the SIP state machine, which may result in an error along the lines of the following:

372The call state should not be IDLE

Workaround: There is no workaround.

- CSCsk04970

Symptoms: There is a memory leak and fragmentation in *Dead* process due to MallocLite. After disabling malloclite, it will be seen as memory allocated to the “Virtual Exec” process in the **show memory allocating-process** [total] command output.

Conditions: The leak occurs whenever the **show vpdn session [l2tp] [all] username username** command is used, and there are many non-matching entries. Memory will be leaked proportional to the number of non-matching usernames (approximately 170 bytes per non-match).

Workaround: Avoid using the **show vpdn session [l2tp] [all] username username** command.

- CSCsk09651

Symptoms: A router crashes while a service policy is being attached, detached, or modified across a virtual template under traffic.

Conditions: This symptom is observed on a Cisco 7200 or Cisco 7301 router that is configured with MLPPP over FR on channelized interfaces.

Workaround: There is no workaround.

- CSCsk10985

Symptoms: IMA group interface does not come up after the reload.

Conditions: This symptom is observed on a Cisco 2811 router with ATM interface that is using VWIC2-2MFT-T1/E1 connected to MGX AUSUM card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface.

- CSCsk15316

Symptoms: When attempting to configure RFC2833 DTMF inband with an MGCP gateway two commands are required:

mgcp dtmf-relay voip codec all mode [nte-calnte-ga] mgcp package-capability fm-package

The “mgcp package-capability fm-package” has been released with Cisco IOS. However, it can only currently be found in the IP Voice Feature Set (ipvoicek9) in either Cisco IOS Release 12.4 or Cisco IOS Release 12.4T.

Conditions: Customers requiring any of the features found in the higher level images (SP Svcs, Adv IP Svcs, Enterprise Svcs), that are not found in the IP Voice feature set, are unable to implement RFC2833 DTMF inband due to the lack of “mgcp package-capability fm-package”.

Workaround: There is no workaround.

- CSCsk19661

Symptoms: In a Cisco 7500 HA router in RPR+ Mode when configuring and unconfiguring channel groups under an E1 controller, the router reports the following:

```
*Aug 22 17:58:34.970: %HA-2-IPC_ERROR: Failed to open peer port. timeout *Aug 22
17:58:34.974: %HA-3-SYNC_ERROR: CCB sync failed for slot: 1 *Aug 22 17:58:34.974:
%HA-5-SYNC_RETRY: Reloading standby and retrying sync operation (retry 1).
and the standby RSP is reloaded.
```

Conditions: This symptom is observed when configuring and unconfiguring channel groups under an E1 controller.

Workaround: There is no workaround.

- CSCsk25405

Symptoms: On a router that is configured as an access or terminal server, high CPU usage may occur because of interrupts, and the following error message and traceback are generated:

```
%SYS-3-NOELEMENT: data_enqueue:Ran out of buffer elements for enqueue -Process=
"<interrupt level>", ipl= 4, pid= 1 -Traceback= 0x41102C3C 0x402F6CDC 0x404AD5D0
0x4025B554 0x4001051C 0x40011668
```

Conditions: This symptom is observed on a Cisco 1800 series, Cisco 2800 series, and Cisco 3800 series that run Cisco IOS Release 12.4(16) and that are configured with an 8-port or a 16-port asynchronous/synchronous high-speed WAN interface card that has an asynchronous connection to another router. The symptom occurs when the other router is reloaded or in boot mode.

Workaround: There is no workaround.

- CSCsk25651

Symptoms: With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM)/CallManager and utilizing SRST functionality, when the IP phones are registered to the SRST router, the message-waiting indication (MWI) states may be incorrect.

Conditions: When a phone registers to a Cisco SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come, first-served fashion. The MWI state, however, is remembered from the previous registration that used that ephone-dn number so the MWI status could be incorrect.

Workaround: Configure both the SRST router and the CUE to use SUBSCRIBE/NOTIFY MWI method.

- CSCsk25778

Symptoms: When a DSPFarm loses IP connectivity to the priority 1 Cisco Unified CallManager (CCM) and fails over to the priority 2 CCM, after a few keepalives the console is flooded with the following error messages when **debug sccp error** is enabled:

```
Aug 13 18:39:35 PDT: sccpold_process_socket_events: Invalid socket
Aug 13 18:39:35 PDT: sccpold_process_socket_events: Invalid socket
Aug 13 18:39:35 PDT: sccpold_process_socket_events: Invalid socket
```

When this occurs, the “Voice Conferenci” process uses excessive CPU, paralyzing the router.

Conditions: This problem was seen in all Cisco IOS versions that have the include the fix for CSCsa70709. This was seen in a customer’s environment and reproducible in the lab with the following setup:

- NM-HDV w/ PVDM-12s as DSPFarm for Conferencing
- Cisco 3725 router
- Any Cisco IOS release that as the fix for CSCsa70709 -Pub/sub CCM cluster running 3.3.5 es51 (also reproduced with CCM 4.1.3 sr2)
- CCM “Station KeepAlive Interval” service parameter set to 10-12 seconds.

Workaround: Downgrade IOS to a version that does not have the fix for CSCsa70709, or set the “Station KeepAlive Interval” parameter to the default of 30 seconds.

- CSCsk26774

Symptoms: Native VLAN information is not included in CDP packets going out ports of an EtherSwitch (ESW) module in Cisco 28xx and Cisco 38xx routers. All the platforms using switchports (of any kind built-in/NM/WIC/HWIC) have this issue: Cisco 8xx, Cisco 17xx, Cisco 18xx, Cisco 26xx, Cisco 36xx, Cisco 37xx, Cisco 28xx, and Cisco 38xx.

Conditions: This symptom causes Cisco IP phone models 7961, 7941 and 7970 that are running SCCP firmware to fail to forward traffic coming from a PC connected at the back of the phone.

Workaround: Enable the “Voice VLAN Access” setting on the phone.

- CSCsk27132

Symptoms: Call is setup using one packetization period and changes mid-call to another packetization after call transfer, causing garbled audio.

Conditions: Occurs when a mid-call state change is required to induce subsequent MGCP modify connections to be sent to the trunking gateway.

Workaround: There is no workaround.

- CSCsk27147

Symptoms: The following SNMP is incorrectly generated:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
This issue is affecting the CISCO-MEMORYPOOL-MIB instead.
```

Conditions: Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

Workaround: Exclude ciscoMemoryPoolMIB from your query with the following commands:
snmp-server view public-view iso included snmp-server view public-view ciscoMemoryPoolMIB excluded Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

- CSCsk35403

Symptoms: Cisco AS5850 sees “400 Active msg is aborted by dlcx”. The Cisco PGW2200 log is full of the following messages:

```
Wed May 23 10:24:14:588 2007 MEST | mgcp-1 (PID 15051) <Error> GEN_ERR_UNKNOWN_MSG:
ip-mgcp-1111PGW001-1[00100003]: Unrecognized or unknown message processMgcpAckFromGW
(no corresponding request) 10 0e 00 04 00 4a 9a b8 00 00 00 99 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 35 00 02 02 03 00 2c 00 04 00 00 01 90 00 2e 00 04 03 dd
d4 bb 00 35 00 1d 41 63 74 69 76
```

Conditions: Occurs when the gateway sends duplicate ACKs for the same transaction ID.

Workaround: There is no workaround.

- CSCsk36559

Symptoms: When one of the T1 or E1 controller NM-HDV2 goes down, the voice calls in the other controller are dropped. This condition relates to interface x/0 x/0/0 (for example, 4/0 causes 4/0/0 to go down).

Conditions: This problem could happen in the MGCP PRI backhauled setup with NM- HDV2.

Workaround: There is no workaround.

- CSCsk40596

Symptoms: Busyout of trunk card with NAS PKG calls removes the trunk card immediately without waiting for calls to drop gracefully.

Conditions: Occurs only on a Cisco AS5400 with MGCP NAS PKG calls.

Workaround: There is no workaround.

- CSCsk42985

Symptom: On a 1841/WIC-1/WIC-1B-U-V2/c1841-adventerprisek9-mz.124-13c combo [hereafter UUT], 180s after BRI interface successfully dials HUB PRI, 1/2 PING packets FAIL from HUB routers destined through UUT to a device on FastEthernet of the UUT, through the CEF switching path.

180 seconds after the ISDN Call from UUT successfully dials HUB PRI, “show adj vi1 internal” changed from point2point(21) to point2point(20) (incomplete) which coincides exactly with the PING failure. It also coincides with the CEF refresh timer triggering.

The direction of the failure is UUT--->HUB router with packets being dropped as “encapsulation failed” in “show ip traffic”.

Conditions: Issues been reproduced on 1841/WIC-1/WIC-1B-U-V2 using legacy DDR on BRI interface. Issue also reproducible in 124-16.14 IOS

Issue is NOT reproducible on 1720/WIC-1B-U/c1700-sy-mz.122-40 combo.

Workaround: Disable CEF switching by configuring “no ip route-cache cef” on BRI0/1/0 and Fa0/1 on “nhtest2”.

- CSCsk44056

Symptoms: Use of the **show voice call status** displays b-channels from 0-22 instead of 1-23 for a T1 configured for PRI.

Conditions: Occurred on a Cisco AS850 Universal Gateway with a T1 configured for “pri-group timeslots 1-24” when H.323/SIP voice calls are made.

Workaround: Use the **show voice call summary** or the **show isdn status** commands to determine the correct b-channel in use.

- CSCsk59662

Symptoms: The **show voice call status** command displays b-channels from 0- 23 instead of 1-24 for a T1 configured for channel associated signaling (CAS).

Conditions: This is seen on a Cisco AS5850 platform for a T1 configured for “ds0-group *e&m-fgb” when H.323/SIP voice calls are made.

Workaround: Use the **show voice call summary** or **show isdn status** to determine the correct b-channel in use.

- CSCsk60281

Symptoms: Outbound call attempts to a group of analog FXO voice-ports which all are members of a trunk-group fail even if there are members which are free to accept inbound or outbound calls.

Conditions: This behavior is observed on Cisco IOS voice routers installed with Cisco IOS Release 12.3(14)T, Cisco IOS Release 12.4 mainline, and Cisco IOS Release 12.4T release trains, using the NM- 1V, NM-2V, or NM-HDA-4FXS with EM-HDA-4FXO and EM2-HDA-4FXO products. It is not observed in Cisco IOS Release 12.3(11)T or earlier releases. Analog FXO voice-ports are configured to operate as members of a trunk-group for dial-plan simplification:

```
! trunk group fxo-tgrp max-calls voice 5 max-retry 5 hunt-scheme round-robin capacity
trunk-group update interval 10 capacity carrier update interval 10 ! voice-port 2/0
trunk-group fxo-tgrp 1 connection plar opx 93922900 ! voice-port 2/1 trunk-group
fxo-tgrp 2 connection plar opx 93922900 caller-id enable ! voice-port 2/2 trunk-group
fxo-tgrp 3 connection plar opx 93922900 ! voice-port 2/3 trunk-group fxo-tgrp 4
connection plar opx 93922900 caller-id enable ! dial-peer voice 9 pots
destination-pattern 9T trunkgroup fxo-tgrp !
```

It has been observed that when inbound calls are received and connected on FXO voice-ports with **caller-id enable** configured, the trunk member is still considered to be available for outbound calls. On the other hand voice-ports without **caller-id enable** set are correctly identified as busy ports and are unavailable for outbound calls. From the **show trunk group EXEC** command it can be seen that the misbehaving ports with CLID enabled report “Free = 1” while the behaving ports without CLID enabled report “Free = 0”. When outbound call attempts are made on ports which are actually busy but reporting “Free = 1” the call fails with a disconnect cause code of 63 (Service or option not available, unspecified).

This problem is observed on the Cisco 2600XM/2691/2800/3700/3800/IAD2430 voice router platforms when the aforementioned voice Network Modules are used. It IS NOT observed on voice Network Modules which use C5510 DSP architecture, such as the NM-HDV2, NM-HD-1V, NM-HD-2V, NM-HD-2VE, and the EVM-HD-8FXS/DID.

Workaround: (1) Disable **caller-id enable** under the voice-ports. (2) Use the traditional dial-plan method of defining one POTS dial-peer per voice-port. (3) Use Cisco IOS Release 12.3(11)T or earlier.

- CSCsk66770

Symptoms: In response to the **fsck ?** command, the USB device is not listed even though it is available.

Conditions: Occurs on USB-enabled routers when a USB device is inserted.

Workaround: There is no workaround.

- CSCsk68927

Symptoms: Cisco VG224 Analog Phone Gateway endpoint rings even after call is answered on another phone

Conditions: Occurs on a VoIP gateway with SCCP/STCAPP controlled analog FXS ports sharing the same DN with another IP phone device. When `fxsls_w_offhook_stop_ringing` is seen while the **no battery-reversal** is configured on the FXS voice port, it is possible to experience this issue with Cisco IOS Release 12.4(5), Cisco IOS Release 12.4(6)T and later releases.

To see the `fxsls_w_offhook_stop_ringing` debug output as shown below, turn on **debug vpm signal**. Turning on debugs on a production IOS router should always been done with care. As a minimum, ensure that console logging is set below the default level of debug with the configuration command **logging console informational**.

```
*Mar 3 01:14:33.067: htsp_process_event: [2/9, FXSLS_WAIT_OFFHOOK,
E_HTSP_STOP_RINGING]fxsls_w_offhook_stop_ringing
*Mar 3 01:14:33.071: 2/9 : ==> Received event:STCAPP_DC_EV_DEVICE_CALL_INFO
*Mar 3 01:14:33.071: 2/9 : Call State:ONHOOK_ML_PENDING
*Mar 3 01:14:33.071: 2/9 : Uninteresting event
*Mar 3 01:14:33.963: [2/9] do_ring_cadence ON->OFF (4000)
*Mar 3 01:14:37.963: [2/9] do_ring_cadence OFF->ON (2000)
*Mar 3 01:14:39.963: [2/9] do_ring_cadence ON->OFF (4000)
*Mar 3 01:14:43.963: [2/9] do_ring_cadence OFF->ON (2000)
*Mar 3 01:14:45.963: [2/9] do_ring_cadence ON->OFF (4000)
*Mar 3 01:14:49.963: [2/9] do_ring_cadence OFF->ON (2000)
*Mar 3 01:14:50.535: 2/9 : stcapp_get_dcb_and_lcb
*Mar 3 01:14:50.535: 2/9 : stcapp_screen_api_event
```

The Cisco VG224 only stops playing the ring cadence once it receives a SCCP message to go ONHOOK.

Workaround: Configure battery reversal under the voice port.

- CSCsk88637

Symptoms: OAM cells are not generated when a new ATM subinterface and PVC is configured. Check subinterface and PVC status and enable the **debug atm oam interface atm/x.x.x** command. Subinterface will be up/up. PVC will be down, and no debug output will be seen.

Conditions: This symptom has been seen in various Cisco IOS 12.4 images.

Workaround: Perform **shut/no shut** commands on ATM subinterface.

- CSCsk94179

Symptoms: When IPv6 prefix delegation (PD) assigns a prefix for virtual access, it create a static route for the prefix in the routing table. However, sometimes it creates incorrect static route for the prefix.

Conditions: The problem is observed when IPv6 PD is configured as a L2TP LNS.

Workaround: There is no workaround.

- CSCsk97384

Symptoms: Abnormally large FreshTime value appears in IVR HTTP client cache entry.

Conditions: This symptom is observed when a VXML voice browser downloads a file from an HTTP server. If the file was modified very recently, the FreshTime for that file may show up with a very large value.

Workaround: There is no workaround.

- CSCsl14635

Symptoms: T38 negotiation is failing for an incoming UPDATE request that has a T38 offer.

Conditions: This symptom occurs when the voice gateway is running Cisco IOS Release 12.4(15)T and is processing incoming Session Initiation Protocol (SIP) calls. When the SIP call is active and an UPDATE request is received that contains a T38 offer, the UPDATE request is rejected. The switchover from voice to fax fails.

Workaround: Fax over T38 works fine when midcall INVITE is used for T38 negotiation.

- CSCsl59294

Symptoms: A Cisco router may see the following error once shortly after bootup:

```
*Nov 21 15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x416DE178
-Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE178 0x416DE650 0x423E303C
0x423E3020 *Nov 21 15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC=
0x416DE188 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE188 0x416DE650
0x423E303C 0x423E3020
```

No functional impact is seen.

Conditions: Occurs on a Cisco 2811 router running Cisco IOS Release 12.4(13d).

Workaround: Disable the following configuration on the router: **voice hpi capture buffersize voice hpi capture destination filename**

- CSCsl71650

Symptoms: Crash in SNASwitch when starting a dlctrace or ipstrace of pdlog that is too large for available memory.

Conditions: Occurs when one of the following conditions is met: 1) A smaller trace is configured and accepted, and then the trace is reconfigured with a buffer size that is too large. 2) A trace is configured with a large buffer size, then snasw is stopped and restarted

If the trace was configured with the *nostart* option, the crash may not occur until the command **snasw tart dlctrace** is issued. Occurs on routers running Cisco IOS Release 12.4(9.9) and later releases, and those running Cisco IOS Release 12.4(9.6)T and later releases.

Workaround: Ensure the buffer size to be configured will fit in the available memory. Use the **show memory summary** command to view the available processor memory. Look in the “Largest(b)” column to see the largest contiguous block of processor memory available. Ensure that block of memory is large enough to hold the buffer size being configured. Remember that the buffer size is specified in kilobytes (K), meaning 16000 is 16000K or 16,384,000 bytes.

Further Problem Description: The following messages may be seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of 65536000 bytes failed from 0x61809390,
alignment 0 Pool: Processor Free: 73041812 Cause: Memory fragmentation Alternate Pool:
None Free: 0 Cause: No Alternate pool -Process= "SNA Switch", ipl= 0, pid= 78
-Traceback= 0x6063C860 0x6078FAA0 0x607946AC 0x60794C48 0x61809398 0x61809A8C
0x61702EB0 0x616EC75C
%SNASW-3-TRACE_2: Resizing of dlctrace buffer failed due to insufficient memory; using
buffer-size of 500 KB.
%ALIGN-1-FATAL: Illegal access to a low address 12:59:14 addr=0x28, pc=0x61809628 ,
ra=0x6180961C , sp=0x6639A4C0
%ALIGN-1-FATAL: Illegal access to a low address 12:59:14 addr=0x28, pc=0x61809628 ,
ra=0x6180961C , sp=0x6639A4C0
TLB (store) exception, CPU signal 10, PC = 0x61809628
```

Wide-Area Networking

- CSCsk39259

Symptoms: The **isdn service nfas_int x b_channel y state z** commands generated in the configuration do not match what is actually entered.

Conditions: For example the following command was entered: **isdn service nfas_int 1 b_channel 3-7 state 2** After which the configuration showed the following: **isdn service nfas_int 1 b_channel 0 state 0**

Workaround: There is no workaround.

- CSCsf10846

Symptoms: The Facility Information Element (FAC IE) in the SETUP message is not received at the other end when the router is configured for E1_NET5 switch type.

Conditions: This symptom is observed in Cisco IOS Release 12.4(7)T1 with the following routers: Cisco 1760 Cisco 2851 Cisco 2651XM Cisco 3745 Cisco 2801 Cisco 3845

Workaround: There is no workaround.

- CSCsi98751

Symptoms: Some B-channels may not be available for Redundant Link Manager (RLM) or IDSN User Adaptation Layer (IUA) usage.

Conditions: Occurs when a partial T1 configuration is entered on the nfas_d primary RLM or IUA DSL.

Workaround: Include B-channel 1 in the configuration.

- CSCsj42852

Symptoms: SNMP linkdown traps are not sent for DS0 serial channels.

Conditions: Occurred after customer moved from Cisco IOS Release 12.2 to Cisco IOS Release 12.4(7c) and moved from Cisco AS5300 to a Cisco AS5350XM.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(16a)

Cisco IOS Release 12.4(16a) is a rebuild release for Cisco IOS Release 12.4(16). The caveats in this section are resolved in Cisco IOS Release 12.4(16a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek78644

Symptoms: SNMP does not use the source address in a VRF.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: Ensure that an SNMP interface is not defined in a VRF.

- CSCsj30317

Symptoms: A FIBDISABLE error message is seen on all VIPs on a Cisco 7500 router.

Conditions: This symptom has been observed when dMPL+QoS is configured on a Cisco 7500 router.

Workaround: There is no workaround.

Interfaces and Bridging

- CSCsi41769

Symptoms: A PVC that is shut down by OAM may continue to receive and forward traffic. This situation causes problems in an APS 1+1 redundancy configuration in which the standby router has a PVC that is shut down by OAM but continues to receive all traffic.

Conditions: This symptom is observed on a Cisco router that has an ATM port adapter.

Workaround: In an IPv4 configuration, shut down the subinterface manually or enter the **ip verify unicast reverse-path** command. In an MPLS configuration, shut down the subinterface manually.

- CSCsi56413

Symptoms: The output may be stuck on a POS interface that is configured for Frame Relay encapsulation. When this situation occurs, the output queue is not emptied, and LMI remains down.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(12) or later. This happens only with very specific hardware configurations including NPE-G1 and PA-POS-OC3SMI. The issue observed when aforementioned Port Adapter is located at slot 4 and not seen with other hardware configurations.

Workaround: Place POS PA in other slot(s). PA location reconfiguration in chassis should fix the problem.

IP Routing Protocols

- CSCek47667

Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

Workaround: There is no workaround.

- CSCek76776

Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCsg55591

Symptoms: When there are link flaps in the network, various PEs received the following error message:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
155:14344:10.150.3.22/32 from 10.2.2.1
```

Or, local label is not programmed into forwarding table for a sourced BGP VPNv4 network.

Conditions: This symptom occurs when an iBGP path for a VPNv4 BGP network is present. A sourced path for the same RD and prefix is brought up after.

Workarounds:

- Remove the iBGP path. If the sourced path comes up first, then the problem will not occur.
- Use different RDs with the different PEs. If the RD+prefix does not match exactly between the iBGP path and the sourced path, the problem will not occur.

- CSCsi32425

Symptoms: A router that is configured for static NAT translations may lose its external/global ARP entry for a NAT address.

Conditions: This symptom is observed when traffic flows run across the router, for example, when the client is outside and server is inside, and when static NAT translation is used for periods of about two minutes.

Workaround: Configure a route map that matches the static NAT translation, and apply the static NAT entry by entering either one of the following commands:

- **ip nat inside source static tcp** *local-ip local-port global-ip global-port* **route-map name** **reversible**

- **ip nat inside source static** *local-ip global-ip* **route-map name** **reversible**

- CSCsi59438

Symptoms: When you enter the **ip multicast limit rpf** command, protection may fail after the RPF link becomes operational.

Conditions: This symptom is observed on a Cisco router that is configured for APS switchover.

Workaround: Clear the state of the corresponding multicast route by entering the **clear ip mroute** command.

- CSCsi62559

Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsj39538

Symptoms: Router tracebacks and then crashes during deconfiguration (removal) of VRF. The following message was seen prior to crash:

```
-Process= "IP RIB Update", ip1= 3, pid= 68
-Traceback= 609538D8 60D1B8B4 612B2838 612588C8 61258CD4 6125E61C 6125ED04
6125EF30 61261CDC 6125A14C 61265A08 6126BE10 6097CF00 609547D8 609548B8
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x609538FC
```

Conditions: No specific conditions are known to cause this fault.

Workaround: There is no workaround.

ISO CLNS

- CSCek76093

Symptoms: A CLNS neighbor may still be formed after the IS-IS protocol has been shut down.

Conditions: This symptom is observed only on serial interfaces.

Workaround: There is no workaround.

- CSCsi57971

Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database on a local router.

Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsj72039

Symptoms: The prefix of a serial interface configured with PPP and passive interface in ISIS will not be part of the ISIS database. This problem can also be seen when the interface is configured as HDLC in place of PPP.

Conditions: This problem is seen with Cisco IOS Release 12.2(18)SXF6 and other releases.

Workaround: See the following workarounds:

- Remove the **passive-interface** command and re-configure it.
- Enter the **clear isis *** command.
- Use any other command that would trigger the ISIS local database generation.

Miscellaneous

- CSCdz55178

Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                        0000000001111111111222222222333^
                        12345678901234567890123456789012|
                                                                |
                                                                PROBLEM
                                                                (Variable Overflowed).
```

Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCin30349

Symptoms: Interface flaps on an ATM IMA port adapter may cause the router to reload.

Conditions: This symptom has been observed when using an PA-A3-8T1IMA/PA-A3- 8E1IMA port adapter on Cisco 7xxx series router platforms. Flaps must be observed or the **shutdown** and **no shutdown** commands must be performed on an applicable interface. However, this symptom is a rare condition, and will not necessarily occur with every flap. This symptom can occur with or without traffic.

Workaround: There is no workaround.

- CSCse59336

Symptoms: MGCP three-way call conferencing may fail because of an abrupt onhook event at the originating endpoint.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) and that is configured for voice calls over Media Gateway Control Protocol (XGCP).

Workaround: There is no workaround.

- CSCsf11944

Symptoms: A router crashes due to the stack for process Exec running low when configuring the **auto qos** command on an ATM subinterface.

Conditions: The symptom has been observed on a Cisco router loaded with Cisco IOS interim Release 12.4(10.5).

Workaround: There is no workaround.

- CSCsg84975

Symptoms: MGCP NAS calls are dropped.

Conditions: This symptom is seen when there are heavy E1 flaps.

Workaround: There is no workaround.

- CSCsh48919

Symptoms: With an ATA flash card, the **dir disk0:** command will fail if any filename or directory name stored on disk0 contains embedded spaces. This applies to disk1 or disk2 as well. This situation can also occur with a compact flash (CF) card using the **dir flash:** command.

Conditions: This symptom has been observed when using a removable flash card, such as an ATA flash card or CF card, that is formatted to use DOSFS. The removable flash card is removed from the router and inserted into a laptop that is running a version of the Microsoft Windows operating system. A "New Folder" directory is created on the flash card and the flash card is removed from the laptop and re-inserted into the router. Entering the **dir** command on the router may fail to show all of the stored files or may crash the router.

Workaround: Remove or rename all files and directories having names with embedded spaces so that no file or directory names contains embedded spaces.

- CSCsh75827

Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the "J" Service-Info attribute), has logged out from the SESM, and then renews its IP address.

Workaround: There is no workaround.

- CSCsh88792

Symptoms: A router that is configured for Dynamic DNS (DDNS) may reload unexpectedly.

Conditions: This symptom is observed when you manually change the IP address of an interface that has DDNS configured.

Workaround: There is no workaround.

- CSCsi51682

Symptoms: The **microcode reload pxf** command does not function.

Conditions: This symptom is observed on a Cisco RPM-XF that runs Cisco IOS Release 12.4 or Release 12.4T and occurs either with the **microcode reload pxf** command or the **microcode reload sar** command. However, the symptom is not platform-specific.

Workaround: There is no workaround.

- CSCsi55964

Symptoms: After a gateway receives a high number of calls, calls may not go through intermittently.

Conditions: This symptom is observed on a Cisco 3800 series that functions as a gateway and that is configured for E1R2 signaling. The symptom occurs when the gateway sends a “clear forward” forward to the PSTN before the PSTN sends a “B1” message.

Workaround: There is no workaround.

- CSCsi57197

Symptoms: The T.37 Fax Offramp process may leak small amounts of memory.

Conditions: This symptom is observed on a Cisco router when the fax call on the PSTN side hangs up before the call completion.

Workaround: There is no workaround.

- CSCsi57927

Symptoms: A Cisco router running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 will show TCP connections hung in CLOSEWAIT state. These connections will not time out, and if enough accumulate, the router will become unresponsive and need to be reloaded.

Conditions: This symptom occurs on a Cisco router running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 when executing a **copy source-url ftp:** command and the FTP server fails to initiate the FTP layer (no banner) but does setup a TCP connection. This may occur when the FTP server is misconfigured or overloaded.

The CLI command will timeout, but will not close the TCP connection or clean up associated resources. The FTP server will eventually answer and timeout itself, and close the TCP connection, but the router will not clean up the TCP resources at this time either.

Workaround: Manually clear TCP resources using the **clear tcp** CLI command, referencing the **show tcp brief** command output.

- CSCsi59685

Symptoms: One-way audio may occur and DTMF digits may not function.

Conditions: This symptom is observed on a Cisco gateway such as a Cisco AS5400 after a SIP transfer has occurred.

Workaround: Enter the **no voice-fastpath disable** command to resolve the one-way audio issue. There is no workaround for the DTMF issue.

- CSCsi84017

Symptoms: When you reload a Cisco 2600 series, the router may hang.

Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsj04563

Symptoms: SSG memory is leaking in Cisco IOS Release 12.4(13b).

Conditions: This symptom occurs when the RADIUS proxy feature is used. Leaking could be triggered on the following call flow scenario:

1. HostObject(HO) with MSID1, ip-address IP1 and username user1@cisco.com is logged on.
2. PDSN sends an acct-stop with MSID1 with session-continue attribute set to TRUE. When this is received, SSG will start a hand-off timer. Note that SSG will not delete the HO at this time.
3. Hand-off timer expires. HO is deleted.
4. SSG now receives an acct-start with MSID1 and username user1@cisco.com.
5.
 - a. SSG will treat this as an auto-domain user, even though auto-domain is not configured on SSG.
 - b. SSG will try to get the profile by extracting the domain name from the structured username and sending an access-req to AAA with username as the domain name.
 - c. Since AAA server does not have the cisco.com profile, it sends an access-reject to SSG.
6. No HostObject is created.

Workaround: There is no workaround.

- CSCsj38829

Symptoms: When running double authentication crypto (ah encap and esp encap auth together) configurations and passing large packet data which requires fragmentation, errored packets can be observed.

Conditions: This symptom has been observed only on routers with AIM-VPN-PLUS AIM cards installed. Routers which support this AIM are the Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 routers.

Workaround: Do not use ESP and AH double authentication. You can use the **no crypto engine accel** command in the configuration to run encryption in the SW engine.

- CSCsj58796

Symptoms: No ringback is generated in calls from VoIP to a PBX end using Cisco Multicast Manager (CMM).

Conditions: This symptom has been observed when a call is made from the VoIP side to the PBX side through an MGCP-controlled CMM.

PBX <-----GW (CMM or Cisco 2620XM) <----CCM <----IP Phone

Workaround: Use a Cisco 2620XM router in place of CMM.

- CSCsj63916

Symptoms: All DATA analog dialout call are setting Bearer Capability to 0x8090 instead of 0x0890A3 (indicating the x-Law) where the A3 suffix is for A-law.

Conditions: This symptom has been observed on a Cisco AS5xxx router running Cisco IOS software later than Cisco IOS Release 12.4(7e) and having to make outgoing DATA calls.

Workaround: Change to Cisco IOS Release 12.4(7e).

- CSCsj97045

Symptoms: While running a Cisco IOS Release 12.4 Mainline release, a Cisco router might crash with a bus error. The error displayed will be similar to:

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x605AFF94

Conditions: This symptom has been observed only if gateway is configured for Voice over IP (VoIP).

Workaround: There is no workaround.

- CSCsk16821

Symptoms: A Cisco router acting as a DHCP server may experience the following problem when Secure ARP is also configured, and the Secure ARP keepalive time is less than the DHCP lease time. If a client device goes into sleep mode for a period of time less than the DHCP server's configured lease time but more than the Secure ARP time, the DHCP lease will be cancelled at the server. If the client awakes, it will have a valid DHCP lease, for the remainder of the last lease time it was granted. When the device awakes and attempts to renew its IP address, it sends a unicast DHCPREQUEST to the DHCP server. Because the lease has been removed from the DHCP server, and there is no ARP entry for the client, the DHCP Server does not send any reply to the device. The Secure ARP feature will, however, prevent the device from communicating until its lease has expired.

Conditions: This symptom has been observed with a Cisco router acting as a DHCP server when Secure ARP is also configured.

Workaround: Disable Secure ARP on the DHCP server or change the Secure ARP keepalive time to correspond to the lease time.

TCP/IP Host-Mode Services

- CSCsh92986

Symptoms: The latency for the **RSH** command could increase when they are flowing through an FWSM module.

Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3 which is not affected by this extra delay issue.

- CSCsi91665

Symptoms: H.323 calls intermittently disconnect.

For each new call the H.323 GW will generate a TCP Port to be used for call setup. Intermittently the GW will generate a TCP Port that is being used for an established connection. When the GW initiates the three way handshake for the new call, it receives a response with an unexpected ACK sequence number. The GW will then send a TCP RST causing the currently established TCP connection/call to be torn down.

Conditions: This problem is observed in both Cisco IOS Release 12.4(13a) and Release 12.4(13b).

Workaround: There is no workaround.

Wide-Area Networking

- CSCee56988

Symptoms: High CPU usage is seen on a Cisco 7301 router.

Tracebacks:

```
Jul  2 21:40:55.973 il: %TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps pointer:
0x0
-Process= "L2X SSS manager", ipl= 0, pid= 69
```

```
-Traceback= 0x606E43DC 0x60B9FAC8 0x60BA11C4 0x619F502C 0x619F4A2C
0x619F4D34 0x619F35C4 0x619F4FF4 0x619F6820 0x619F5ED8 0x619F6350 0x619CA1F4
0x619CA6C4 0x619D2524 0x619CABB4 0x619CAFA0
```

Conditions: This symptom has been observed with Cisco IOS Release 12.4(5b) on a Cisco 7301 router with PPTP/VPDN connections after the CU is moved from RATE- LIMIT to MQC policy-based limiting of the customer's bandwidth.

Workaround: There is no workaround.

- CSCek56693

Symptoms: An ALIGN-3-SPURIOUS message is seen on the console.

Conditions: This symptom has been observed when ATM PVC is deactivated and the PVC is carrying PPPoA sessions.

Workaround: Deactivate the PPPoA sessions before deactivating the PVC.

- CSCsi69009

Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase "cloned from: AAA, AAA, ..." (that is, multiple instances of AAA) as identification.

Workaround: There is no workaround.

Further Problem Description: You can alleviate the situation somewhat by configuring the NCP Timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

- Increase the hello timers for L2TP and for the receive windows.
- Configure the timers under the virtual template.
- Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
- Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

- CSCsi74960

Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

Workaround: There is no workaround.

- CSCsj45426

Symptoms: Cisco AS5850 feature boards crash.

Conditions: This symptom occurs when giving the **no pri-group timeslots** command.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(16)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(16). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(16). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCeb20967

Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S, 12.1(14)E4, or 12.2 S when the following sequence of events occurs:

1. A packet is switched via Cisco Express Forwarding (CEF).
2. The egress interface has queueing/shaping configured.
3. The egress interface is congested, causing the packet to be placed into the hold queue.

Workaround: There is no workaround.

- CSCek58338

Symptoms: A router may crash because of memory corruption in the chunk memory.

Conditions: This symptom is observed on a Cisco 7600 series when both the Embedded Resource Manager (ERM) and Bidirectional Forwarding Detection (BFD) are configured. The symptom is platform-independent.

Workaround: Disable BFD.

- CSCek69519

Symptoms: When the execution of the **show aaa user all** command waits at the "More" prompt and when you cancel the command, the console is locked up for up to one minute and the CPU usage increases to near 100 percent during this time.

Conditions: This symptom is observed on a Cisco router that is configured with many broadband sessions.

Workaround: There is no workaround.

- CSCsd27777

Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCsf12539

Symptoms: Tracebacks may be generated for all accounting messages.

Conditions: This symptom is observed on a Cisco router that is configured for AAA.

Workaround: There is no workaround.

- CSCsg69244

Symptoms: After you have performed a microcode reload on a router, a ping may not go through for 100 percent.

Conditions: This symptom is observed on a Cisco router that has an RSP after you have entered the **microcode reload** command.

Workaround: There is no workaround.

- CSCsh44174

Symptoms: After a router has crashed, another crash may occur while the crashinfo is being generated, and a traceback with memory addresses is displayed.

Conditions: This symptom is observed on a Cisco router when, during the crash, the data in key memory locations is written to a crashinfo file on the bootflash device of the router.

Workaround: Specify an alternate storage device to store the crashinfo in the startup configuration, for example, by adding the following line to the startup configuration:

exception crashinfo disk0:

- CSCsh49291

Symptoms: When you remove an IPSLA tcpConnect or udpEcho responder by using the CLI via one Telnet terminal session while, via another Telnet terminal session, the **show ip sla monitor responder** command is executed, the router may crash, although this occurs rarely.

Conditions: This symptom is observed only when the display of the output of the **show ip sla monitor responder** command on the second terminal is extremely slow.

Workaround: There is no workaround.

- CSCsh63542

Symptoms: The following SNMP error message and tracebacks are seen:

```
SEC 8:000049: Jan 31 22:25:00.760: %SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe
regn with SNMP by driver having ifIndex 709 and ifDescr Tunnel0
-Traceback= 204128 204230 92DB90 92DF6C B2CF8C BBF368 BC00C8 1C4EFC 1C5524
1C60B8 1C655C 2EC5CC
```

Conditions: This symptom has been observed when new interfaces are added (or existing interfaces like tunnel come up) after bootup, or when new or existing interfaces come up after RPR+ switchover when running Cisco IOS Release 12.0 (32)S6. Also, this symptom occurs if the **snmp ifindex persist** command is configured on the router.

Workaround: There is no workaround.

Further Problem Description: Though customer traffic is not affected, this symptom does impact the SNMP stats and other SNMP data for both the original and the new interface. Usually the message is from the standby RP, so once that standby RP becomes active, the data from SNMP polls of these interfaces would not be accurate.

- CSCsh76038

Symptoms: AAA enable authentication via a TACACS+ server fails.

Conditions: This symptom occurs when the **aaa authentication enable default group tacacs+** command or the **aaa authentication enable default group** command pointing towards a TACACS+ server group is configured.

Workaround: There are two possible workarounds.

1. On the TACACS+ server, configure a user named "\$enab{x}\$", where {x} is the desired privilege level, such as using "\$enab15\$" for regular enable mode. This user's password will be the enable password.
2. Change to a Cisco IOS release that does not yet include CSCin98780.

Further Problem Description: When using a RADIUS server, enable authentication is done by authenticating a user named "\$enab{x}\$". When using a TACACS+ server, enable authentication is done by using the user's actual username, which allows TACACS+ to define separate enable passwords for each user.

CSCin98780 erroneously caused the Cisco IOS software to authenticate "\$enab{x}\$" as a username for enable authentication for TACACS+ servers. This causes enable authentications in existing installations to fail, since TACACS+ server user databases do not normally contain a "\$enab{x}\$" user. This fix, CSCsh76038, corrects the issue, and any Cisco IOS release with this fix will transmit the user's actual username again in any enable authentication request.

- CSCsi04892

Symptoms: When you enter the **no ip sla schedule operation-number** command, error messages may be generated.

Conditions: This symptom is observed on a Cisco router when you unconfigure an Ethernet SLA feature.

Workaround: There is no workaround.

- CSCsi13312

Symptoms: Authentication with Security Device Manager (SDM) 2.3.3 fails, preventing you from logging into the router through HTTPS, HTTP, SSH, Telnet, console, or any management application.

Conditions: This symptom is observed on a Cisco router that is fresh out of the box and affects the following routers:

Cisco 800 series

Cisco 1700 series

Cisco 1800 series

Cisco 2700 series

Cisco 2800 series

Cisco 3700 series

Cisco 3800 series

Workaround: For extensive information and a workaround, see the following Field Notice:

http://www.cisco.com/en/US/products/ps5855/products_field_notice09186a0080809c8e.shtml

- CSCsi49008

Symptoms: SNMP requests on VRFs may time out, and the SNMP response is sent back to a 0.0.0.0 address.

Conditions: This symptom is observed only for SNMP requests that enter via a VRF.

Workaround: There is no workaround.

IP Routing Protocols

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCsc46018

Symptoms: When a call is made between Cisco CallManagers that involve the RSVP agent, the router on which the RSVP agent is configured may crash and generate tracebacks.

Conditions: This symptom is observed when the RSVP agent uses the loopback interface as the source interface, that is, RSVP is configured on the loopback interface.

Workaround: Do not configure RSVP on the loopback interface. Rather, configure RSVP on one of the physical outgoing interfaces.

- CSCsh02161

Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

Workaround: There is no workaround.

- CSCsh20140

Symptoms: A small memory leak may occur when ISPF is enabled. When you deconfigure OSPF, the following error message and traceback are generated:

```
%SYS-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk
30E3268.
-Process= "Exec", ipl= 0, pid= 3,
-Traceback= 0x69F968 0x813670 0x8137C4 0xD57928 0xD6A230 0xB37824 0xB38550
0x6E33F0 0x706EBC 0x7ABDD0 0x7ABDCC
```

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsb38978. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb38978>. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: Do not configure ISPF.

- CSCsh42565

Symptoms: Traffic engineering (TE) tunnels go down when an intermediate link has the **ip ospf network non-broadcast** command enabled.

Conditions: This symptom is observed in an OSPF network over TE tunnels that are established on non-broadcast links.

Workaround: Do not use non-broadcast links. Rather, use another OSPF network type. If this is not an option, there is no workaround.

- CSCsh51559

Symptoms: The following error message may be generated on a router that is configured for VPN or VPNv4:

For VPN: ALIGN-3-SPURIOUS: Spurious memory access made at bgp_vpn_afmodify_walk

For VPNv4: ALIGN-3-SPURIOUS: Spurious memory access made at bgp_vpnv4_afmodify_walk

Conditions: This symptom is observed on a Cisco router that is configured for BGP and IPv4 in a VRF address-family configuration and that imports routes from a VRF.

Workaround: There is no workaround. However, the error message is of a cosmetic nature and can be ignored.

- CSCsh80678

Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(22) or a later release when the **auto-summary** command is enabled for BGP.

Workaround: Enter the **no auto-summary** command.

- CSCsh90153

Symptoms: Connectivity is lost through a router when traffic is processed twice by NAT.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(8a), that is configured for NAT and PBR, and that has a firewall feature enabled. Under certain conditions, traffic is processed twice by NAT when it does not need to be.

Workaround: Remove the firewall configuration from the router.

Further Problem Description: Syslogs and the output of the **show ip nat translation** command show that traffic that is processed twice by NAT does not traverse the router.

- CSCsi35947

Symptoms: When you enter the **ip nat outside source static {tcp | udp} global-ip global-port local-ip local-port** command, the command is not accepted.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.11).

Workaround: There is no workaround.

- CSCsi84089

Symptoms: A router crashes by bus error a few seconds after OSPF adjacencies go up.

Conditions: This symptom has been observed on an ISR configured with OSPF running Cisco IOS Release 12.0S, Release 12.2S, Release 12.2SX, Release 12.2SRA, Release 12.2SRB or Release 12.4 images, but not in Release 12.2SRC or Release 12.3 images.

Workaround: Add area 0 in the OSPF VRF processes, or the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

Workaround: There is no workaround.

ISO CLNS

- CSCsf26043

Symptoms: IS-IS protocol packets may not be classified as high-priority. When this situation occurs during stress conditions and when the IS-IS protocol packets are mixed with other packets, the IS-IS protocol packets may be dropped because of their low-priority.

Conditions: This symptom is observed on a Cisco platform that is configured for Selective Packet Discard (SPD).

Workaround: Ensure that DSCP rewrite is enabled and then enter the following command:

```
mls qos protocol isis precedence 6
```

- CSCsh63324

Symptoms: The following error message may be generated when IS-IS is configured:

```
%SYS-2-CHUNKPARTIAL: chuck name ISIS NSF cp ch
```

Conditions: This symptom is observed on a Cisco router that functions in an MPLS configuration when the **nsf cisco** command is configured under the **router isis** command.

Workaround: There is no workaround. However, the error message appears to be of a cosmetic nature and does not appear to affect the functionality of the router.

Miscellaneous

- CSCds25257

Symptoms: A gatekeeper rejects new registration requests from a Cisco Unified CallManager (CUCM) or other H.323 endpoints with Registration Rejection (RRJ) reason of duplicateAlias. Attempting to clear this stale registration fails and a "No such local endpoint is registered, clear failed." error message is generated.

Conditions: This symptom is observed in the following topology:

CUCM H.225 trunks register to a gatekeeper (GK) cluster. Gatekeeper 1 (GK1) and gatekeeper 2 (GK2) are members of the GK cluster. The CUCM registers first to GK1, then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

When the H.225 trunk attempts to register with GK1, it is rejected because the alternate registration is still present, and there is no way to clear it.

```
10.9.20.3          34273 10.9.20.3          32853 SJC-LMPVA-GK-1    H323-GW A
ENDPOINT-ID: 450FC24400000000 VERSION: 5 AGE: 1618993 secs
SupportsAnnexE: FALSE
g_supp_protos: 0x00000050
H323-ID: SJC-LMPVA-Trunk_4
```

Workaround: Reset the gatekeeper by entering the **shutdown** command followed by the **no shutdown** command, or reboot the affected GK.

- CSCec38904

Symptoms: A call from a remote client may be terminated at a Layer 2 Tunneling Protocol (L2TP) network server (LNS) that functions as a multihop node instead of being forwarded to a second LNS.

Conditions: This symptom is observed when the L2TP Tunnel Connection Speed Labeling feature is enabled in a multihop-node configuration in which an LNS functions as a multihop node that authenticates a user based on the connection speed of the user. When the connected Cisco Access Registrar (ARS) RADIUS server sends an Access-Accept message, the LNS should forward the L2TP session to a second LNS, but does not do so, causing the call to be terminated on the LNS itself.

Workaround: There is no workaround.

- CSCed13843

Symptoms: Pings fail across PPPoE.

Conditions: This symptom occurs when a Cisco 7500 series router has distributed switching enabled.

Workaround: Disable dCEF on the Cisco 7500 core router or enable a feature that causes the packets to be punted to the RP. Note that CEF works fine.

- CSCed90732

Symptoms: Windows VPN Client Version 4.0.3 fails to enroll with the Cisco IOS CA server using SCEP. Other devices (PIX, IOS) enroll successfully. VPN Client does get the CA certificate installed but not the user certificate. It gives the error message:

```
error 42: unable to create certificate enrollment request
```

```
The client log shows:
```

```
Could not find data portion of HTTP response from CEP server. Contact your CA administrator for further instructions.
```

Conditions: This symptom has been observed when enrolling Windows VPN Clients with Cisco IOS routers acting as CA servers.

Workaround: Enroll via a PKCS10 request.

- CSCej42879

Symptoms: A traceback may be generated when packets are transmitted over a basic IPSec connection between two peers in transmission mode and tunnel mode using multilink interfaces.

Conditions: This symptom is observed on a Cisco 3845 that runs Cisco IOS Release 12.4(5).

Workaround: There is no workaround.

- CSCek38201

Symptoms: A router may reload or display an alignment traceback when you enter the **show crypto socket** command.

Conditions: This symptom is observed on a Cisco router that has an OSPFv3 IPsecv6 configuration.

Workaround: There is no workaround. To prevent the symptom from occurring, do not enter the **show crypto socket** command in an OSPFv3 IPsecv6 configuration.

- CSCek44049

Symptoms: Spurious memory accesses may occur on the CPU of the active PRE of a Cisco 10000 series when sessions are brought up, when a disk is accessed, and when you reload the standby RP. When this situation occurs, the following error message is generated:

%ALIGN-3-SPURIOUS: Spurious memory access made at[ifs_copy_file_common
(0x6069ca34)+0x904]

Conditions: This symptom is observed on a Cisco 10000 series that has 12,000 PPPoEoA sessions.

Workaround: There is no workaround.

- CSCek60527

Symptoms: An AAA server does not authenticate.

Conditions: This symptom is observed on a Cisco platform that functions as an AAA server and that runs Cisco IOS Release 12.3(13) when you dial up using Microsoft callback through an asynchronous line. Dialup through an ISDN modem works fine.

Workaround: There is no workaround.

- CSCek63384

Symptoms: A service policy is unexpectedly removed.

Conditions: This symptom is observed when you apply a service policy to a multilink interface and then the interface is reset.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the service policy after the multilink interface has been brought up.

- CSCek65491

Symptoms: A router that is configured for HA may unexpectedly reload because of a spurious memory access.

Conditions: This symptom is observed on a Cisco 10000 series when an L2TP tunnel interface flaps, causing a spurious memory access in the chunk memory. Note that the symptom is platform-independent.

Workaround: There is no workaround.

Further Problem Description: Note that SSO is not supported on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds and that is configured for broadband aggregation:

"In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+), and Stateful Switchover (SSO). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only."

For more information, see the Broadband Aggregation and Leased-Line Overview document:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_chapter09186a00805057de.html

- CSCek67814

Symptoms: The *bandwidth* argument of the **ip rtp priority starting-rtp-port-number port-number-range bandwidth** interface configuration command does not appear when you enter the **show running-config** command.

The same situation may occur for the **ip rtp reserve lowest-udp-port range-of-ports [maximum-bandwidth]** command.

The rest of the command is correctly displayed and the bandwidth value that is stored internally is correctly set at 0.

Conditions: This symptom is observed when the *bandwidth* argument (or *maximum-bandwidth* argument) is configured as 0. If any other valid value is configured, it will correctly appear in the output of the **show running-config** command.

Workaround: There is no workaround.

- CSCek71514

Symptoms: On a Cisco router that has the **mpls ldp igp sync delay delay-time** command enabled, the master timer may be accessed prior to being initialized, and the following error message is generated:

```
%SYS-3-MGDTIMER: Uninitialized timer, init with uninitialized master, timer =
53E62C0.
-Process= "Init", ipl= 0, pid= 3
```

Because the master timer was not properly initialized, other symptoms may occur, including the following:

- When the LDP session comes up, further error messages and a traceback regarding the master timer may be generated:

```
LDP-SYNC: Et1/0: Delay notifying IGP of sync achieved for 60 seconds R1
(config)#
%SYS-3-MGDTIMER: Uninitialized timer, set_exptime_internal, timer = 198A980.
-Process= "Tag Control", ipl= 0, pid= 61
-Traceback= 2AEAE4 3642DC 364580 364ADC 364BAC 9BF154 9C22C0 9C24D8 9D4500
9CD544 9D1C8C 34AD58 34AD54
```

- When the "Delay notification" error message is generated (see above), the output of the **show mpls ldp igp sync** command may show "0 seconds left" for the synchronization delay time, which contradicts the "Delay notification" error message:

```
R1#show mpls ldp igp sync
Ethernet1/0:
  LDP configured; LDP-IGP Synchronization enabled.
  Sync status: sync achieved; peer reachable.
  Sync delay time: 60 seconds (0 seconds left)
  IGP holddown time: infinite.
  Peer LDP Ident: 192.168.1.2:0
  IGP enabled:
```

- OSPF may remain in the "sending maximum metric" state, and the routing table may not be updated, as can be shown in the output of the **show ip ospf mpls ldp interface** command:

```
R1#show ip ospf mpls ldp interface
Ethernet1/0
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Required
  Holddown timer is not configured
  Interface is up and sending maximum metric
```

Conditions: These symptoms are observed when an RPR+ switchover has occurred or when you configure the **mpls ldp igp sync delay delay-time** command while LDP is not enabled or while LDP is enabled but not fully active (for example, when all the interfaces are down).

Workaround: There is no workaround to prevent the initial error message and traceback from being generated. However, after the initial error message and traceback have been generated, you can prevent any further symptoms from occurring by reconfiguring the synchronization timer and re-enabling the **mpls ldp igp sync delay delay-time** command on the affected interface as in the following example:

```
R1(config-if) no mpls ldp igp sync delay
R1(config-if) mpls ldp igp sync delay 60
R1(config-if) no mpls ldp igp sync
R1(config-if) mpls ldp igp sync
```

- CSCsa80126

Symptoms: The SNMP IfIndex Persistence feature may not function as expected. The ifIndex table that is created when you enter the **snmp-server ifindex persist** command is not loaded when the router boots and the indexes of all interfaces are reassigned in a sequential order that depends on the interface number.

Conditions: This symptom is observed on a Cisco router when you first create a subinterface with a sequence number that is lower or in between the numbers of the existing interfaces and then you reload the router.

Workaround: There is no workaround.

- CSCsb15138

Symptoms: The following error messages may be generated on a gateway that functions in a configuration in which 80 channels are processed by a VXML Server, and the call may be dropped:

```
//-1//HTTTPC:/httpc_streaming_create: attempt to create a session with id 699
while this id is in use
//2144684/0BCEFB9AA28/VXML:/vxml_media_done:
CALL_ERROR; fail with vapp error 2, protocol_status_code=0
//2144684/0BCEFB9AA28/VXML:/vxml_media_done:
CALL_ERROR; *** error.badfetch.http.0 event is thrown
```

Conditions: This symptom is observed rather rarely on a Cisco AS5400 gateway when the HTTP client session IDs range from 1 to 2048 because of the socket limit per Cisco IOS process. The error messages are generated when the HTTP client attempts to create a new session with the same ID as an old session that is still in use. In this situation, only a benign warning message should be generated, and the call should be accepted. If an HTTP streaming session remains in use for a long time and the traffic load of the gateway is high, the symptom is more likely to occur.

Workaround: Configure an event handler as in the following example:

```
<catch event="error.badfetch.http.0">
<!-- Actual event handler goes in here -->
</catch>
```

If this is not an option, the symptom may be mitigated by disabling IVR streaming mode via the **ivr prompt streamed none** command.

- CSCsb46223

Symptoms: A router may crash because of a bus error when several Telnet users simultaneously run Tcl scripts. The problem is exacerbated by using scripts that take a long time to complete such as the following Tcl script:

```
set ver [exec "show tech-support"] puts $ver
```

When two users connect to the router through Telnet sessions and run the above Tcl script at the same time, the router may crash.

Conditions: This symptom is observed when the Tcl scripts send text to the Telnet sessions simultaneously.

The symptom may also occur when a single user connects to the router through a Telnet session, then from this Telnet session establishes another Telnet session into the same router, and runs a Tcl script that produces text output.

Workaround: Prevent multiple users from connecting to the router through Telnet and running Tcl scripts. In such a situation, ensure that users do not enter commands in Tcl scripts that may take a long time to display their output such as the **show tech-support** command.

Further Problem Description: Router console connections and incoming SSH connections to the router are not affected.

- CSCsb60279

Symptoms: A CPUHOG condition followed by a software-forced crash may occur on a mobile home agent.

Conditions: This symptom is observed when the mobile users or bindings increase to a very large number.

Workaround: There is no workaround.

- CSCsc61309

Symptoms: When DHCP for IPv6 is configured on an interface, memory may not be freed when a packet is dropped, causing memory allocation failures.

Conditions: This symptom is observed, for example, when the interface is not configured for IPv6, when the interface is not in the up state, or when encryption is configured on the interface.

Workaround: There is no workaround.

- CSCsc86541

Symptoms: Packets are not forwarded through the intermediate router in a three-router topology.

Conditions: This symptom is observed when three routers are connected serially. After you have configured IP addresses on all the connected interfaces, packets from the first router are not forwarded through the intermediate router to the last router but are dropped on the intermediate router.

Workaround: There is no workaround.

- CSCsd27617

Symptoms: IKE negotiation fails with a wrong group preshared key.

Conditions: This symptom is observed on a Cisco router that has an eight character key such as "cisco123" that is defined under the EzVPN group configuration and occurs after you have entered the **password encryption aes** command.

Workaround: To prevent the symptom from occurring, do not use an eight character key under the EzVPN group. After the symptom has occurred, re-enter the group and key.

- CSCsd75161

Symptoms: BRI-secured telephone endpoints are disconnected after the call is connected.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(7.24)T but may also affect Release 12.4.

Workaround: There is no workaround.

- CSCsd78066

Symptoms: When a packet is sent to a multicast address by using a socket API over UDP, the packet is forwarded over the interfaces that do not belong to the VRF that is set on the socket.

Conditions: This symptom is observed on a Cisco router that is configured for VRF-lite and that has a VRF set on the socket.

Workaround: There is no workaround.

- CSCsd81407

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCse40423

Symptoms: A tunnel interface cannot ping the other end of an IP tunnel.

Conditions: This symptom is observed when ATM is configured and when the tunnel interface is up.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface.

- CSCse99958

Symptoms: A Cisco router may fail to access a flash card after formatting it, and the following error message is generated:

```
*** Emulating mis-aligned load at 0x80000190 PC = 0x8001179c ... succeeded
```

Conditions: The symptom is observed on a Cisco 7200 series, Cisco 7301, and Cisco 7500 series that run Cisco IOS Release 12.4(10) or Release 12.4(12) and occurs only when a flash card is accessed from the ROMmon prompt.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(8a) or an earlier release.

- CSCsf07232

Symptoms: Tcl standard I/O operations such as a **puts** command may not display text on the terminal line under which the Tcl code is running. The text may be displayed on the terminal line that was the first one to connect (for example, vty0) or may not be displayed anywhere. Both print to standard output (STDOUT) and standard error (STDERR) streams are affected.

Conditions: This symptom is observed on a Cisco router when more than one user is logged into a device, when one user enters Tcl Shell mode via the **tclsh** command, and then a second user enters Tcl Shell mode.

Workaround: Ensure that only one user is connected to the device when Tcl standard I/O operations are run. If this is not an option, there is no workaround.

Further Problem Description: When Tcl standard I/O operations are run on vty0 with only one user logged in, the text is displayed correctly.

- CSCsf08998

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsf13044

Symptoms: The outgoing interface (OIF) for bidirectional PIM multicast routes is not updated properly because PIM joins are not received through the MDT tunnel.

Conditions: This symptom is observed on a Cisco 7600 series that has Gigabit Ethernet interfaces that are configured for dCEF. Note that the symptom is platform-independent.

Workaround: There is no workaround.

- CSCsf27267

Symptoms: A router that functions as an IPIPGW may not forward an "225 NON STD" message to the terminating gateway.

Conditions: This symptom is observed on a Cisco 2691 that runs Cisco IOS interim Release 12.4(10.4)T but may also affect other platforms and Release 12.4. The symptom occurs when a call is made from an IP phone in a topology in which the IPIPGW is located in between a Cisco CallManager and an H.323 gateway. When the call is put on hold, the IPIPGW receives an "H225 NON STD" message that includes a "callPreserve False" notification but does not forward this message to the terminating gateway. Similarly, when the call is resumed, an "H225 NON STD" message that includes a "callPreserve True" notification is not forwarded.

Workaround: There is no workaround.

- CSCsf28509

Symptoms: When you enter the **clear ip dhcp binding** command to clear DHCP bindings, the corresponding DHCP-initiated subscriber sessions are not cleared.

Conditions: This symptoms is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Enter the **clear ip subscriber** command to clear the subscriber sessions.

- CSCsg37484

Symptoms: A router may reload because of a bus error in a crypto map and generate the following error message:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x4284A878
```

Conditions: This symptom is observed on a Cisco router that has an IPSec crypto map.

Workaround: There is no workaround.

- CSCsg59326

Symptoms: When an ATM (that is, a cash machine, not a WAN platform) is connected to a switch service module, significant packet loss may occur.

Conditions: This symptom is observed on a Cisco 2800 series router.

Workaround: Change the Ethernet speed to 10 Mbps at both ends.

- CSCsg61561

Symptoms: STRING.TCP signatures that contain min-match-length parameters are limited to 16 instances. Signatures of this type do not compile correctly after 16 signatures have been reached, failing to generate an alarm. The only way to determine a signature failure is to test the signature with the proper attack traffic. The signature display does not indicate when these signatures have failed to compile properly.

Conditions: This symptom is observed on a Cisco platform that has IPS configured on one or more interfaces with STRING.TCP signatures present.

Workaround: Test and determine a signature failure. Search the signature file for STRING.TCP signatures that contain min-match-length parameters. Delete working signatures in order for failing signatures to compile correctly. Compilation occurs in the order in which signatures are defined in the signature definition file.

- CSCsg69022

Symptoms: A router may crash when you enter the **no telephony-service** command while the running configuration is being generated.

Conditions: This symptom is observed rarely and occurs because of a race condition between the execution of the **no telephony-service** command and the generation of the running configuration.

Workaround: There is no workaround.

- CSCsg69644

Symptoms: You may not hear a busy tone when you call a busy off-net number.

Conditions: This symptom is observed on a Cisco platform such as a Cisco IAD 2400 series that runs Cisco IOS Release 12.4 and that has ground start signaling configured.

Workaround: There is no workaround.

- CSCsg70474

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsg73595

Symptoms: On a router that is configured as an access or terminal server, high CPU usage may occur because of interrupts, and the following error message and traceback are generated:

```
%SYS-3-NOELEMENT: data_enqueue:Ran out of buffer elements for enqueue
```

```
-Process= "<interrupt level>", ipl= 4, pid= 1
```

```
-Traceback= 0x60E652FC 0x602A8A4C 0x6012D8F0 0x600B1688 0x6257EC58 0x60048114
```

Conditions: This symptom is observed on a Cisco 1800 series, Cisco 2800 series, and Cisco 3800 series that run Cisco IOS Release 12.4(10) and that are configured with an 8-port asynchronous/synchronous high-speed WAN interface card (HWIC-8A/S-232) that has an asynchronous connection to another router. The symptom occurs when the other router is reloaded or in boot mode.

Workaround: There is no workaround.

- CSCsg83834

Symptoms: A router may crash and generate an "%ALIGN-1-FATAL: Illegal access to a low address" error message.

Conditions: This symptom is observed on a Cisco router that is configured for IPv6, IPsec, and multicast.

Workaround: There is no workaround.

Further Problem Description: The fix for caveat CSCsg83834 also fixes caveat CSCsg94837. For more information about caveat CSCsg94837, see

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg94837>.

- CSCsg87559

Symptoms: A client that has IPv6 for DHCP implemented may not receive a correct prefix.

Conditions: This symptom is observed on a Cisco 7200 series that functions as a DHCP server, that has IPv6 for DHCP implemented, and that has the **allow-hint** DHCP IPv6 interface server configuration enabled. Note that the symptom is platform-independent.

Workaround: There is no workaround.

- CSCsh11993

Symptoms: When a Demilitarized Zone (DMZ) port is configured on a router, autoinstall does not function.

Condition: This symptom is observed on a Cisco 830 series that runs Cisco IOS Release 12.4 or Release 12.4T when you use Fast Ethernet (FE) port 0, port 1, port 2, or port 3 instead of port 4 that is linked to the Ethernet 2 interface that is used as the DMZ port. The Ethernet 2 interface receives the IP address via DHCP, but because FE port 4 is in the down/down state, autoinstall does not function.

The following is an example of the configuration:

```
AUTOINSTALL: Ethernet2 is assigned <ip add 1>
AUTOINSTALL: Obtain tftp server address (opt 150) <ip add 2>

!
interface Ethernet0
  no ip address
  shutdown
!
interface Ethernet2
  ip address dhcp
end
```

When the symptom occurs, the output of the **show ip interface brief** shows the following:

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet1	unassigned	YES	unset	down	down
FastEthernet2	unassigned	YES	unset	up	up

FastEthernet3	unassigned	YES	unset	down	down
FastEthernet4	unassigned	YES	unset	down	down
Ethernet0	unassigned	YES	unset	administratively down	down
Ethernet2	<ip add 1>	YES	DHCP	down	down

Workaround: Use FE port 4 that is linked to the Ethernet 2 interface and that is used as the DMZ port.

Further Problem Description: For information about the DMZ port, see the Demilitarized Zone (DMZ) Port document:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide09186a0080235e23.html

- CSCsh22469

Symptom 1: For POTS-to-POTS calls between an originating analog voice port over a PRI trunk that are terminating on another voice port, call attempts fail because the outgoing ISDN Q.931 SETUP has an incorrect Bearer Capability:

```
ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16 is 0x0 0x0, Calling
num 123456789
ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16 is 0x0 0x0, Called
num 987654321
ISDN Se0/0/0:15 Q931: TX -> SETUP pd = 8 callref = 0x497A
Sending Complete
Bearer Capability i = 0x9090
Standard = CCITT
Transfer Capability = 3.1kHz Audio
Transfer Mode = Circuit
Transfer Rate = 64 kbit/s
Channel ID i = 0xA98383
Exclusive, Channel 3
Progress Ind i = 0x8183 - Origination address is non-ISDN
Calling Party Number i = 0x0080, '123456789'
Plan:Unknown, Type:Unknown
Called Party Number i = 0x80, '987654321'
Plan:Unknown, Type:Unknown
Dec 7 12:54:12.660: ISDN Se0/0/0:15 Q931: RX <- RELEASE_COMP pd = 8
callref
= 0xC97A
Cause i = 0x82C131903980 - Bearer capability not implemented
Display i = 'BEARER CABABILITY NOT IMPLEMENTED'
```

The correct Bearer Capability for the E1 PRI should be 0x9090A3 for G.711 A-law. For a T1 PRI, the correct Bearer Capability should be 0x9090A2 for G.711 u-law.

Symptom 2: The same issue may occur with an outgoing Q.931 SETUP that has an incorrect Bearer Capability on VoIP-to-POTS calls when the PRI voice port has the **bearer-cap speech** command configured.

Conditions: This symptom is observed on a Cisco voice gateway that runs a Cisco IOS software image that integrates the fix for caveat CSCsf20569. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf20569>. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected.

The symptom occurs when a voice call originates at an analog POTS interface and travels over a PRI trunk. Note that when the originating voice port is a digital POTS trunk or an EFXS (CME/SRST ephone) POTS interface, there is no corruption of the bearer-cap in the outgoing Q.931 SETUP.

The symptom may also be observed on regular VoIP-to-POTS call scenarios when the **bearer-cap speech** command is configured on the PRI voice port.

There are no known scenarios in which a bearer-cap problem occurs for an incoming call on a PRI voice port.

Workaround: There is no workaround. Note that the symptom does not occur in Cisco IOS releases up to Release 12.4(12) and up to Release 12.4(11)T.

- CSCsh26382

Symptoms: IPsec SAs may be unexpectedly deleted.

Conditions: This symptom is observed on a Cisco router when the transform set that is used to create IPsec tunnels is a combination of both AH and ESP protocols.

Workaround: Do not use a combination of AH and ESP protocols for the transform set. Use either the AH protocol or use the ESP protocol.

- CSCsh30879

Symptoms: The CPU usage may suddenly increase up to 99 percent and the platform may crash. When this situation occurs, the Inspect Timer process uses more than 95 percent of the CPU and remains at that level even after the traffic has stopped.

Conditions: This symptom is observed when you enter the **clear ip ips configuration** command while traffic is being processed.

Workaround: There is no workaround.

- CSCsh33430

Symptoms: A traceback may occur in an HSRP function and the platform may reload unexpectedly.

Conditions: This symptom is observed on a Cisco platform that has the HSRP Support for ICMP Redirects feature enabled and occurs when a learned HSRP group is removed after a resign message has been received.

Workaround: Disable the Support for ICMP Redirects feature by entering the **no standby redirects** global configuration command.

- CSCsh39318

Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

```
%MROUTE-4-ROU TELIMIT (x1): [int] routes exceeded multicast route-limit of
[dec] - VRF [chars]
```

Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

Workaround: There is no workaround.

- CSCsh44798

Symptoms: An MGCP endpoint may become stuck and generate the following error message:

```
400 previous message in progress
```

Conditions: This symptom is observed when a call agent sends a CRCX message, either before receiving the acknowledgement for the previous DLCX message from the gateway or before acknowledging the previous DLCX message from the gateway.

Workaround: There is no workaround.

- CSCsh48788

Symptoms: You cannot make an outbound call from an IP phone that is connected to a Cisco Unified CallManager Express router. When you pick up the phone to make a call, the phone display indicates "offhook" but there is no dial tone. An error message is generated at the debug level in the log that indicates that the call is already reserved. Inbound calls work fine.

When the symptom occurs, a spurious memory access is generated and the output of the **show voice vtsp call** command shows that some resources remain in the "S_SETUP_REQ_FAIL" state.

Conditions: This symptom is observed when an incoming H.323 "signonly call" is received for the IP phone in the following topology:

A PBX that is configured for Q.SIG is connected to a Cisco 2800 series that functions as a gateway and that runs Cisco IOS Release 12.4. In turn, this gateway is connected via an H.323 link to the Cisco Unified CallManager Express router. The PBX sends a "signonly call" (for example with message-waiting indications [MWIs]) to the IP phone extension.

Workaround: There is no workaround.

- CSCsh49391

Symptoms: Local diagnostics may not function on a T1/E1 daughter card of a Communication Media Module (CMM).

Conditions: This symptom is observed when the CMM boots and affects CMM software images with DSPware 4.4.21 release and above. This means that Cisco IOS interim Release 12.4(11.1), Release 12.4(7d), Release 12.4(8b), Release 12.4(10a) and later releases are affected.

Workaround: There is no workaround.

- CSCsh51293

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of Cisco IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

- CSCsh55982

Symptoms: When you enter the **shutdown** command twice on an interface of a router, the interface on the peer shows that it is up, that is, the link is in the up/up state and the LED lights up.

Conditions: This symptom is observed on onboard Gigabit Ethernet interfaces of a Cisco 3800 series and Cisco AS5400 and does not occur on other platforms.

Workaround: Do not enter the **shutdown** command on an interface that is already shut down.

- CSCsh58082

Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>.

- CSCsh58729
Symptoms: A router that is configured for MPLS FRR may crash.
Conditions: This symptom is observed on a Cisco 7600 series but is platform-independent.
Workaround: There is no workaround.
- CSCsh59375
Symptoms: A DHCP interface may not be switched when you enter the **ip dhcp smart-relay** command.
Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(12.15a) and that is configured for MPLS VPN.
Workaround: There is no workaround.
- CSCsh60966
Symptoms: SNASw generates a Last Message Fault Error(FFFF0306).
Conditions: SNASw attached PU is including Control Vectors on its Bind Response, although the Bind Response sent by the SNASw attached PU has the Control Vector Bit turned off (Byte 7 Bit 6).
Workaround: There is no workaround.
- CSCsh62418
Symptoms: ISDN does not come up and remains in "TE1 Assigned" state instead of entering the "Multiple Frame Established" state.
Conditions: This symptom is observed on a Cisco 7200 series after you have performed a physical OIR of a PA-VXC-2T1E1+ port adapter.
Workaround: Reload the router.
- CSCsh64365
Symptoms: A ping does not yield a 100-percent result after you have entered the **no set-overload-bit** for an IS-IS configuration.
Conditions: This symptom is observed on a Cisco 7200 series but is not platform-specific.
Workaround: There is no workaround.
- CSCsh70638
Symptoms: During system bootup or bursty traffic, the following error messages might be seen:

```
00:20:16: %ALIGN-SP-STDBY-3-SPURIOUS: Spurious memory access made at
0x72AB2370 reading 0xB8
00:20:16: %ALIGN-SP-STDBY-3-TRACE_SO: -Traceback= (s72033-
adventerprisek9_wan_dbg-0-dso-bn.so+0x1AE370) ([42:0]+0x1AE47C) ([31:-3]3-dso-
b+0x220994) ([41:0]+0x220FB8) ([41:0]+0x221A90) ([41:0]+0x22214C) ([41:0]
+0x222D6C) ([41:0]+0x2233CC)
```

Conditions: This symptom has been observed with bursty IPC traffic during system booting up or switching over, typically with heavy configuration data exchanges.
Workaround: There is no workaround.
- CSCsh71247
Symptoms: Cisco Express Forwarding (CEF) may not function correctly over PPP sessions, and the output of **show adjacency** command shows information similar to the following:

```
Protocol Interface Address IP Virtual-Access3 point2point(8) (incomplete)
```

Conditions: This symptom is observed on a Cisco router when PPP is used on a full virtual-access interface or multilink bundle.

Workaround: Disable CEF.

- CSCsh74975

Symptoms: A router may reload or a leak memory may occur when UDP malformed packets are sent to port 2517.

Conditions: This symptom is observed on a Cisco router that functions as a VoIP dial peer and that is configured for H.323.

Workaround: There is no workaround.

- CSCsh78054

Symptoms: "IP Local Pool Trap" messages for high and low notification do not include the length field for the specific pool name in each object of the trap, while an SNMP get/walk command does collect the length field for the specific pool and shows it properly.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4.

Workaround: Configure the **ip local pool** command with high and low threshold values, as in the following example:

```
Router(conf t)#ip local pool <pool-name> <ip-low> <ip-high> threshold <low> <high>
```

- CSCsh91470

Symptoms: RTP dynamic payload types may not be classified.

Conditions: This symptom is observed on a Cisco router that is configured for NBAR and that has a class-map configuration when the **match protocol rtp payload-type** *payload-string* command is enabled with "96-126" as the *payload-string* argument. This command does not detect any matching packets.

Workaround: There is no workaround.

- CSCsh92914

Symptoms: A router may unexpectedly reload when you attempt to open a reversed SSH connection by using the SSHv1 protocol.

Conditions: This condition is observed on a Cisco router that runs Cisco IOS Release 12.4.

Workaround: Force the SSH transport to be SSHv2 by entering the **ip ssh version 2** global configuration command.

- CSCsh94526

Symptoms: When an acct-stop message is received for a non-RADIUS proxy user (that is, a normal IP user), a router that is configured for SSG crashes.

Conditions: This symptom is observed when SSG is configured for RADIUS proxy mode and when the **ssg wlan reconnect** command is enabled.

Workaround: There is no workaround.

- CSCsh97579

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

- CSCsi04183

Symptoms: A router that is configured as an EasyVPN client is not able to auto connect to the EasyVPN server using its saved Xauth username/password.

Conditions: This symptom is observed when the router is powered-up or when the ISAKMP re-keying happens.

Workaround: Manually execute the **crypto ipsec client ezvpn xauth** command in the router console and enter the respective username/password.

- CSCsi04538

Symptoms: A router that is configured as a Cisco Unified Call Manager Express (CUCME) router may crash because of a memory corruption.

Conditions: This symptom is observed when voice calls are made involving a transcoder.

Workaround: There is no workaround.

- CSCsi04707

Symptoms: Configuring an AUX port for async interface through a non-slotted notation such as the **interface async 1** command or slotted notation such as the **interface async x/y/z** command may not be possible on a Cisco 2851.

Conditions: This symptom has been observed on a Cisco 2851 router with Cisco IOS Release 12.4(13). This symptom has not been seen on Cisco IOS Release 12.4 (10) and earlier.

Workaround: There is no workaround.

- CSCsi08756

Symptoms: The ringback tone level that is played on a platform that is configured for use in a country in Europe may be very low compared to the ITU specification, which states that tones should be nominal -10dBm0.

Conditions: This symptom is observed on a Cisco AS5400XM.

Workaround: There is no workaround.

- CSCsi10157

Symptoms: When you associate and then disassociate a VRF from a tunnel source interface, a DMVPN spoke may crash.

Conditions: This symptom is observed only when a VRF is configured on a tunnel interface.

Workaround: There is no workaround.

- CSCsi21922

Symptoms: A VC and a traffic engineering (TE) tunnel are not in a state that you would expect.

Conditions: This symptom is observed when you configure MPLS TE along with a pseudowire.

Workaround: There is no workaround.

- CSCsi22483

Symptoms: A router that is configured for VXML may crash at the "vxml_keyword_get" function.

Conditions: This symptom is observed during a stress test with a VXML script that uses the "tts-voice-profile" property.

Workaround: Remove the "tts-voice-profile" property from the VXML script.

- CSCsi24939

Symptoms: A router may reload unexpectedly when using a CA that does not support the GetCAPS exchange (part of SCEP), because of a bus error crash after entering the **crypto ca authenticate** command.

Any response other than a real GetCAPS reply will cause the crash. Before the router crashes, the following error messages and traceback are generated:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Crypto CA.
-Traceback= 0x42AB7410 0x424A6E18 0x42469B7C 0x424651E0
%Software-forced reload
```

```
Preparing to dump core...
```

```
%CRYPTO-4-IKMP_NO_SA: IKE message from xxx.xx.xx.x has no SA and is not an
initialization offer
```

Conditions: This symptom is observed on a Cisco 2821 that runs Cisco IOS Release 12.4(10b) but may not be platform-specific.

Workaround: There is no workaround.

- CSCsi27767

Symptoms: One-way audio may occur when a call is transferred or picked up after having been on hold.

Conditions: This symptom is observed intermittently on a Cisco Communication Media Module (CMM) for calls that are transcoded because of a transfer or being placed on hold and for which the RTP stream terminates on the CMM.

The symptom appears to occur because of a significant change in the sequence numbers and timestamp of the RTP packets while the same SSRC is kept. You can identify this situation with a packet capture of the RTP stream.

Workaround: There is no workaround.

- CSCsi42086

Symptoms: A memory leak may occur on a router that is configured for SSG when unsupported 3GPP attributes are received by SSG.

Conditions: This symptom is observed when SSG is configured to function in RADIUS proxy mode.

Workaround: Ensure that the unsupported 3GPP attributes are removed by filtering them before a RADIUS packet is received by SSG.

- CSCsi42490

Symptoms: A Cisco 3700 series with an IMA interface may crash.

Conditions: This symptom is observed when the ATM IMA PVC had an AutoQoS configuration.

Workaround: Remove the AutoQoS configuration.

- CSCsi60004

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsi62152

Symptoms: A Cisco router that is configured for IPSec HA may generate a "SYS-2-CHUNKMALLOCFAIL" error message and a traceback.

Conditions: This symptom is observed on a Cisco 3845 that functions as an EzVPN server. The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCsi78118

Symptoms: Traceback can be seen at "iphc_decompress".

Conditions: This symptom has been observed in Cisco IOS interim Release 12.4 (13.13)T1.

Workaround: There is no workaround.

- CSCsi99217

Symptoms: When 6000 L2TP sessions are disconnected, a Cisco IOS LNS router is stuck on High CPU Utilization (99% or 100%) with PPP IP Route process for 5 minutes.

Conditions: This symptom has been observed under stress test conditions (thousands sessions are disconnected at once) with no traffic and using Cisco IOS Release 12.4(13). This symptom has not been observed on earlier releases.

Workaround: There is no workaround.

- CSCuk61773

Symptoms: CPU spikes may occur on a router that is configured for Web Cache Communication Protocol (WCCP) earlier than Release 4.0.7.

Conditions: This symptom is observed on a Cisco 7600 series when WCCP is in communication with a Cisco Wide Area Application Services (WAAS) appliance. Note that the symptom is platform-independent.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsh36234

Symptoms: File paths that start with a double slash may fail to open the file successfully.

Conditions: This symptom is observed when you enter the **install** command with the **scp** keyword, that is when an SCP application functions as the source.

Workaround: Move the file to another location where the double slash is not required.

Alternate Workaround: Use another protocol such as RCP or TFTP to transfer the file.

- CSCsi40766

Symptoms: H.323 calls on a Cisco IOS VoIP gateway may fail after the gateway has processed about 54,500 calls.

Conditions: This symptom is observed when H.323 uses TCP to transport signaling messages. When the Cisco IOS gateway must generate a unique port for the local TCP session, this port is selected from a range of open ports. When the number of times that a unique TCP session is created for the same IP address on the gateway exceeds 54,500, further attempts to create a local TCP port fail and calls are not completed.

The symptom occurs for H.323 calls only when a separate TCP session is established for the H.245 session. When H.245 tunneling is enabled or no H.245 session is established, the symptom does not occur for H.323 calls.

When the **debug ip tcp transaction** command is enabled on the gateway, the "TCP: Ran out of ports for network 0" debug output is generated when the symptom occurs.

Enabling debugs on a Cisco IOS gateway should always be done with caution to minimize impact to the performance of the router. As a minimum, ensure that logging to the console is changed from the default behavior of the debug level to, for example, an informational level.

Workaround: After the symptom has occurred, reload the Cisco IOS VoIP gateway. To prevent the symptom from occurring, ensure that for H.323 call processing all H.323 devices have H.245 tunneling enabled. This may not always be possible: for example, H.245 tunneling on Cisco CallManager is not supported.

Wide-Area Networking

- CSCek67875

Symptoms: During a test of a B-Channel Maintenance Procedure (BCAC), an incoming SERVICE message is not printed with the correct channel.

Conditions: This symptom is observed when a collision occurs between a SERVICE message and a SETUP message.

Workaround: There is no workaround.

- CSCsc28674

Symptoms: Incorrectly charged units are shown in the output of the **show call calltracker** command and the calltracker data that is requested via SNMP.

Conditions: This symptom is observed on a Cisco AS5350 gateway that runs Cisco IOS Release 12.3(16).

Workaround: There is no workaround.

- CSCsf30493

Symptoms: When a T.37 onramp call is made, the following error message may be generated:

```
%CSM-3-NO_VDEV: No modems associated
```

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS interim Release 12.4(10.7). The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCsg89222

Symptoms: A PPP session that is initiated from a client may not be forwarded. to an LNS.

Conditions: This symptom is observed on a Cisco router after the PPP session has been established.

Workaround: Enter the **vpdn source-ip** global configuration command.

- CSCsh00185

Symptoms: A software forced-crash occurs with a memory corruption in the processor pool memory.

Conditions: This symptom is observed on a Cisco router that is configured for ISDN and that has an unusually long calling name with more than 70 characters in the received Facility IE.

Workaround: There is no workaround.

- CSCsh06841

Symptoms: A router may crash while establishing a PPP session.

Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsh75479

Symptoms: A platform that is configured for ISDN may crash because of a bus error when you shut down an ISDN interface.

Conditions: This symptom is observed on a Cisco platform when traffic is being processed on the interface while you shut down the interface.

Workaround: There is no workaround.

- CSCsh82513

Symptoms: The output of the **show isdn active** command may show disconnected calls.

Conditions: This symptom is observed on a Cisco router when analog modem calls are made after a normal ISDN digital call has been made.

Workaround: There is no workaround.

- CSCsh85902

Symptoms: When a normal ISDN call is disconnected, a DISCONNECT message is issued. The content of this DISCONNECT message is replaced with the content that is explicitly configured. This configured message may have an invalid facility component. When this situation occurs, the receiving side should send a facility reject component, but this does not occur.

Conditions: This symptom is observed on a Cisco router that is configured with a PRI and that runs Cisco IOS interim Release 12.4(12.15)T. The symptom may also occur for Release 12.4 and other 12.4T releases.

Workaround: There is no workaround.

- CSCsi13337

Symptoms: The count of the CCB value at the interfaces for the primary and backup channel may be incorrect, and the count of the available B-channels may also be incorrect.

Conditions: This symptom is observed on a Cisco platform after you have entered the **isdn test 12 disconnect** command on the interface for the backup D-channel.

Workaround: There is no workaround.

- CSCsi14053

Symptoms: When a gateway responds to a request for information (for example, "CC_INFO_REQ:Ux_InfoReq(nlcb)") from a service provider with an information message for incoming calls, the service provider releases the call with a message similar to the following one:

```
Q931: RX <- RELEASE pd = 8 callref = 0x00B2
Cause i = 0x82E2 - Message not compatible with call state or not implemented
```

Conditions: This symptom is observed when a Cisco platform that runs Cisco IOS Release 12.4(9)T2 or Release 12.4(11)T1 dials into a third-party vendor switch via a PRI.

Workaround: There is no workaround.

- CSCsi18698

Symptoms: When a NOTIFY message is forwarded by a terminal gateway to the ISDN side, the NOTIFY message may be incorrectly decoded.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.11), interim Release 12.4(13.5)T, or interim Release 12.4(13.8)T.

Workaround: There is no workaround.

- CSCsi21853

Symptoms: When you attempt to change the ISDN T306 timers, the changes are not accepted.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4.

Workaround: There is no workaround.

Further Problem Description: The ISDN T306 configuration updates the values of the ISDN T307 timers.

- CSCsi27449

Symptoms: A Non-Facility Associated Signaling (NFAS) configuration with a back-to back PRI connection may fail and an "L3_GetUser_NLCB EVENT 0X2 No NLCB 2" error message may be generated, that is, a ping from the client to the router mail fail.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.11) when an interface is configured as a dialer interface.

Workaround: There is no workaround.

- CSCsj10593

Symptoms: The trunking gateway (TGW) crashes when checked for gateway interconnect functionality for SETUP messages with all PRI switch types from User to NT side.

Conditions: This symptom has been observed with Cisco IOS interim Release 12.4 (15.6). This symptom occurs when the **isdn test call interface Serial1:23 22222** command is entered at the Call Starter and with Switch Types: OGW: primary-ni TGW: primary-dms100.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(13f)

Cisco IOS Release 12.4(13f) is a rebuild release for Cisco IOS Release 12.4(13). The caveats in this section are resolved in Cisco IOS Release 12.4(13f) but may be open in previous Cisco IOS releases.

- CSCsg16778

Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

Workaround: There is no workaround.

Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- CSCsh49391

Symptoms: Local diagnostics may not function on a T1/E1 daughter card of a Communication Media Module (CMM).

Conditions: This symptom is observed when the CMM boots and affects CMM software images with DSPware 4.4.21 release and above. This means that Cisco IOS interim Release 12.4(11.1), Release 12.4(7d), Release 12.4(8b), Release 12.4(10a) and later releases are affected.

Workaround: There is no workaround.

- CSCsh51293

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of Cisco IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

- CSCsj74812

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: Occurs when running **show** commands on an exec session that has been established through one of the integrated modems on a WIC-AM or WIC-2AM. This would only be seen on asynchronous cards with gt96k, HWIC or PQUICC drivers.

Workaround: There is no workaround.

- CSCsj85065

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>.

- CSCsk27147

Symptoms: The following SNMP is incorrectly generated:

```
%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
```

This issue is affecting the CISCO-MEMORYPOOL-MIB instead.

Conditions: Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the SNMP process takes 5-20% of the CPU load.

Workaround: Exclude ciscoMemoryPoolMIB from your query with the following commands:

```
snmp-server view public-view iso included snmp-server view public-view
```

```
ciscoMemoryPoolMIB excluded
```

Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

- CSCsk40676

Symptoms: The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Conditions: Occurs when LZS compression is used on a Windows Vista client.

Workaround: Disable LZS compression.

- CSCsk42759

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsk61790

Symptoms: Syslog displays password when copying the configuration via FTP.

Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

Workaround: There is no workaround.

- CSCsk62253

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

- CSCs132142

Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with “Bad getbuffer” error may also be reported.

Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCs134303

Symptoms: Cisco 7200 router crashes when unconfiguring service policy from Multilink Frame Relay (MFR) interface.

Conditions: Occurs if one of the MFR bundle link interfaces was previously being used for Multilink PPP over Frame-relay. Changing the encapsulation may not clean up queuing configuration properly - a dual first in first out (FIFO) queue may remain on the interface.

Workaround: Ensure a dual FIFO queue is not present on MFR bundle link interface. It should be plain FIFO queue. If it is a dual FIFO, change the interface to HDLC encapsulation, which should remove the dual FIFO queue, then back to MFR bundle link encapsulation.

- CSCs162609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCs170143

Symptoms: Under heavy traffic, ISDN calls may be rejected due to high CPU usage with the following messages seen in the log (with tracebacks):

```
%IVR-3-LOW_CPU_RESOURCE: IVR: System experiencing high cpu utilization (98/100). Call (callID=23524) is rejected.
```

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (32/18),process = ISDN.
```

Conditions: This problem occurs only under heavy traffic.

Workaround: There is no workaround.

- CSCs171540

Symptoms: Router reloads when the **show ip bgp options** command is entered.

Conditions: This is seen in releases where CSCsj22187 is fixed.

Workaround: There is no workaround.

- CSCs183415

Symptoms: After executing the following CLI (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

Test 10 :

1. clear ip bgp 10.0.101.46 ipv4 multicast out
2. clear ip bgp 10.0.101.47 ipv4 multicast out

Test 1:

3. show ip bgp ipv4 multicast nei 10.0.101.2
4. show ip bgp ipv4 multicast [<prefix>]
5. config t

Crash does not happen for each of the following cases:

1. if same CLI is cut-paste manually, there is no crash.
2. if **clear cli** is not executed, there is no crash.
3. if **config term** is not entered, there is no crash.

Conditions: The symptom occurs after executing the above CLI.

Workaround: There is no workaround.

- CSCs187400

Symptoms: H323 setup message is malformed after NAT translation

Conditions: Setup message includes the neededFeatures, desiredFeatures, supportedFeatures extensions.

Workaround: Do not use the extensions listed above.

- CSCsm04442

Symptoms: Delete an interface which has ip summary-address rip configured. The router crashes.

Conditions: In the scenario where different summary addresses are configured for different interfaces, if we delete an interface that has a summary-address configuration which is the last one for that summary-address that it leads to.

Workaround: Remove the **ip summary-address rip** configuration from an interface which is going to be deleted.

- CSCsm08291

Symptoms: Virtual access interfaces flap, and the following error message is displayed:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done.
```

Conditions: Occurs on a Cisco 7206VXR with NPE-G2 and running Cisco IOS Release 12.4.(11)T1.

Workaround: There is no workaround.

- CSCsm08398

Symptoms: Negative number is displayed in the output for the **show ip nat translation command and in rate limiting. This limit entry option fails due to the huge number of entries shown in ip nat statistics.**

Conditions: In some situations **show ip nat statistic** calculation falls negative, which shows as huge number by the NAT. Limit entry looks into this number for stop NAT translation. When this is negative limit entry stops NAT from doing translations.

Workaround: There is no workaround.

- CSCsm17879

Symptoms: After putting the onboard GE0/0-1 interfaces into promiscuous mode, they still will not accept packets with destination MAC other than the broadcast and the interface MAC.

Conditions: This affects the onboard GE interfaces only.

Workaround: Use FE/GE ports from a module to achieve this, if available.

- CSCsm45113

Symptom: Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

Conditions: The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

Workaround: Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB. instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Further problem description: The **clear ip route *** command can correct the routing table until the next poll of ipRouteTable MIB.

- CSCso15151

Symptoms: When Multicast Distributed Fast Switching is configured, a VIP crashes on a Cisco 7500 router that is running a Cisco IOS 12.3 release.

Conditions:

1) The router has around 1000 interfaces/subinterfaces. 2) Distributed multicast is configured. 3) The router is running any Cisco IOS 12.3 release.

Workaround: There is no workaround.

Further Problem Description: In summary, the line card is accessing the memory location that has been freed already. This results in the VIP crashing. There are sanity checks that are missing in Cisco IOS 12.3 releases. The problem is similar to what bug CSCdm29808 does on line cards of the Cisco 12000 Internet series router (this router does not support Cisco IOS Release 12.3). This basically checks if the interface index on MDfS messages is less than the MDfS Idb map size, which indicates the current size of the Idb map table.

Resolved Caveats—Cisco IOS Release 12.4(13e)

Cisco IOS Release 12.4(13e) is a rebuild release for Cisco IOS Release 12.4(13). The caveats in this section are resolved in Cisco IOS Release 12.4(13e) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCir01027

Symptoms: SNMP over IPv6 does not function.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCsg02387. A list of the affected releases can be found at

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg02387>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Use SNMP over IPv4.

- CSCsj30317

Symptoms: A FIBDISABLE error message is seen on all VIPs on a Cisco 7500 router.

Conditions: This symptom has been observed when dMPL+QoS is configured on a Cisco 7500 router.

Workaround: There is no workaround.

- CSCsk70446

Cisco IOS emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

A traceback appears after the error message. This traceback is encountered with long URLs.

It is important to note that this error message does not imply that packet data is corrupted. However, it does provide an early indicator of other conditions that can eventually lead to poor system performance or a Cisco IOS restart.

IP Routing Protocols

- CSCek76776

Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCse04220

Symptoms: The BGP table version remains stuck at 1, and the router may crash.

Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for a network service access point (NSAP) address family.

Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

- CSCsj09838

Symptoms: When the BGP session between a Route Reflector (RR) and PE router flaps, the RR may no longer send some routes to the PE router.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsi85222. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi85222>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **clear ip bgp * all in** command on the PE router to retrieve all routes from the RR.

- CSCsj39538

Symptoms: Router tracebacks and then crashes during deconfiguration (removal) of VRF. The following message was seen prior to crash:

```
-Process= "IP RIB Update", ipl= 3, pid= 68
-Traceback= 609538D8 60D1B8B4 612B2838 612588C8 61258CD4 6125E61C 6125ED04
6125EF30 61261CDC 6125A14C 61265A08 6126BE10 6097CF00 609547D8 609548B8
```

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0x609538FC
```

Conditions: No specific conditions are known to cause this fault.

Workaround: There is no workaround.

- CSCsk35985

Symptoms: The system crashes when the **show ipv6 ospf lsdb- radix** hidden command is entered.

Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

Miscellaneous

- CSCdz55178

Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                                000000000111111111122222222333^
                                12345678901234567890123456789012|
                                                                |
                                                                PROBLEM
                                                                (Variable Overflowed).
```

Workaround: Change the name of the cable QoS profile to a length that is less than 32 characters.

- CSCeg20335

Symptoms: A Cisco 10000 series may lose the PVC configurations for several subinterfaces and high CPU usage may occur. When you attempt to reconfigure the PVCs, error messages similar to the following may be generated:

```
Router#pvc 35/134
Unable to create PVC 35/134 on ATM1/0/0.10350134. Possibly multiple users
configuring IOS simultaneously
Further info about other user:
Process id: 42, Process: Slot 1/0 CMD Process, TTY: 0, Location: Console
Router(config-subif)#
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(7)XI1 or Release 12.2(27)SBB.

Workaround: Reload the router.

- CSCek60527

Symptoms: An AAA server does not authenticate.

Conditions: This symptom is observed on a Cisco platform that functions as an AAA server and that runs Cisco IOS Release 12.3(13) when you dial up using Microsoft callback through an asynchronous line. Dialup through an ISDN modem works fine.

Workaround: There is no workaround.

- CSCek63384

Symptoms: A service policy is unexpectedly removed.

Conditions: This symptom is observed when you apply a service policy to a multilink interface and then the interface is reset.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the service policy after the multilink interface has been brought up.

- CSCek71877

Symptoms: IPv6 pings are not working when the **atm route-bridged ipv6** command is configured on the UUT.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(13.5)T images.

Workaround: There is no workaround.

- CSCek75633

Symptoms: A router may crash when you attach a VC class to an ATM bundle.

Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

Workaround: There is no workaround.

- CSCse59336

Symptoms: MGCP three-way call conferencing may fail because of an abrupt onhook event at the originating endpoint.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) and that is configured for voice calls over Media Gateway Control Protocol (XGCP).

Workaround: There is no workaround.

- CSCsf11944

Symptoms: A router crashes due to the stack for process Exec running low when configuring the **auto qos** command on an ATM subinterface.

Conditions: The symptom has been observed on a Cisco router loaded with Cisco IOS interim Release 12.4(10.5).

Workaround: There is no workaround.

- CSCsg37484

Symptoms: A router may unexpectedly reload because of a bus error.

Conditions: This symptom can be observed on a Cisco router that has an IPSec crypto map. CSCsg37484 was reported by customer running:

1. dynamic cryptomap
2. DPD is enabled

Workaround: There is no workaround.

- CSCsg87559

Symptoms: A client that has IPv6 for DHCP implemented may not receive a correct prefix.

Conditions: This symptom is observed on a Cisco 7200 series that functions as a DHCP server, that has IPv6 for DHCP implemented, and that has the **allow-hint** DHCP IPv6 interface server configuration enabled. Note that the symptom is platform-independent.

Workaround: There is no workaround.

- CSCsg91306

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsh22725

Symptoms: Outbound calls fail on a MGCP-controlled CAS channel on a Cisco VoIP gateway.

Conditions: This symptom is observed when the following conditions occur:

- A timeslot on an E&M T1 trunk is taken out of service from the connected switch side, showing as a permanent inbound seizure. In this situation, the output of the **show voice call summary** command indicates that the status for this channel is “EM_PARK”.
- A Cisco CallManager that interworks with the Cisco VoIP gateway checks the status of the trunk via an MGCP AUEP command. The gateway responds with an “ES: rlc” message, which indicates that the trunk is available for calls.

Because the reported availability and actual availability of the channel are mismatched, all outbound calls on the channel fail.

Workaround: Attempt to clear the out-of-service state from the connected switch side. If this is not possible, when interworking with the Cisco CallManager, first enter the **shutdown** command followed by the **no shutdown** command on the voice port and then enter the same commands on the T1 controller. Doing so causes the gateway to send an NTFY message that indicates that there is an inbound seizure on the channel.

- CSCsh30879

Symptoms: The CPU usage may suddenly increase up to 99 percent and the platform may crash. When this situation occurs, the Inspect Timer process uses more than 95 percent of the CPU and remains at that level even after the traffic has stopped.

Conditions: This symptom is observed when you enter the **clear ip ips configuration** command while traffic is being processed.

Workaround: There is no workaround.

- CSCsh48919

Symptoms: With an ATA flash card, the **dir disk0:** command will fail if any filename or directory name stored on disk0 contains embedded spaces. This applies to disk1 or disk2 as well. This situation can also occur with a compact flash (CF) card using the **dir flash:** command.

Conditions: This symptom has been observed when using a removable flash card, such as an ATA flash card or CF card, that is formatted to use DOSFS. The removable flash card is removed from the router and inserted into a laptop that is running a version of the Microsoft Windows operating system. A “New Folder” directory is created on the flash card and the flash card is removed from the laptop and re-inserted into the router. Entering the **dir** command on the router may fail to show all of the stored files or may crash the router.

Workaround: Remove or rename all files and directories having names with embedded spaces so that no file or directory names contains embedded spaces.

- CSCsh64365

Symptoms: A ping does not yield a 100-percent result after you have entered the **no set-overload-bit** for an IS-IS configuration.

Conditions: This symptom is observed on a Cisco 7200 series but is not platform-specific.

Workaround: There is no workaround.

- CSCsh74975

Symptoms: A router may reload or a leak memory may occur when UDP malformed packets are sent to port 2517.

Conditions: This symptom is observed on a Cisco router that functions as a VoIP dial peer and that is configured for H.323.

Workaround: There is no workaround.

- CSCsi21922

Symptoms: A VC and a traffic engineering (TE) tunnel are not in a state that you would expect.

Conditions: This symptom is observed when you configure MPLS TE along with a pseudowire.

Workaround: There is no workaround.

- CSCsi29174

Symptoms: On a Cisco IOS voice gateway, the tx and rx counters in the output of the **show call active voice brief** command may not function properly. The counters may not increment at all or may increment in bursts every 10 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7c), Release 12.4(7d), Release 12.4(8c), or Release 12.4(13a).

Workaround: There is no workaround.

- CSCsi77147

Symptoms: DTMF path confirmation is not received for a SIP call.

Conditions: This problem is due to an issue with the SIP state machine, which may result in an error along the lines of the following:

```
00:05:10: //-1/xxxxxxxxxxxx/SIP/Error/sipSPISipIncomingMsg: Invalid method for
(STATE_IDLE): ACK
```

The call state should not be IDLE.

Workaround: There is no workaround.

- CSCsi81891

Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

Workaround: There is no workaround.

- CSCsi83724

From enclosure: Release-note

From enclosure: Release-note

Symptoms: Ping between CE routers fails, after flapping PE routers interface or flapping ip cef on PE routers.

Conditions: This symptom occurs when ATM PVC adjacency between PE and CE becomes incomplete when interface or ip cef is flapped on PE routers.

Workaround: There is no workaround.

- CSCsi84767

Symptoms: A T38 fax outbound to the Cisco AS5850 fails.

Conditions: After upgrading from Cisco IOS Release 12.3(11)T9 to Cisco IOS Release 12.4(7e), it is observed that fax calls from an analog Cisco IAD2420 or Cisco IAD2430 outbound to the Cisco AS5850 fail. It appears the Cisco AS5850 is having trouble falling back from T38 to passthrough. Standard configuration is T38 enabled on the Cisco AS5850 but not on the analog IAD. Disabling T38 on the Cisco AS5850 results in successful faxing.

Workaround: There is no workaround.

- CSCsj08606

Symptoms: A VWIC2-2MFT-T1/E1 may stay in alarm state after either shut/ no shutting the controller or removing and replacing the interface cable.

Conditions: The controller is configured as follows:

```
controller E1 0/0/0
 framing NO-CRC4
 ds0-group 0 timeslots 16 type ext-sig
 ...
 ds0-group 30 timeslots 30 type ext-sig
 alarm-trigger blue 0
```

The problem has been observed in the c3845-spservicesk9-mz.124-9.T3 image.

Workaround: Shut/no shut the controller or remove and replace the cable a second time.

- CSCsj27183

Symptoms: H323-->SIP interworking fails for a Fast start call when transcoding is enabled on an IPIPGW. Transcoding is done between G711ulaw and G729r8 codecs.

Conditions: This failure is seen for H323--SIP--SIP--SIP and H323--SIP--SIP-- H323 call flows when transcoding is enabled on IPIPGW1. It is also seen on H323--H323--H323--SIP call flow for transcoding on IPIPGW2. This is seen only with a Fast Start call (both with H245 Tunnel enabled and disabled), and the call passes with a slow start call.

Workaround: There is no workaround.

- CSCsj37709

Symptoms: Memory held by mem_mgr_chunk_t and mem_mgr_mempool_t in dead process is causing an out-of-memory condition on the gateway.

Conditions: This scenario occurs when SIP phone calls are made using the default application or a TCL IVR application and the **header-passing** command is enabled in voice service VoIP SIP configuration mode.

The following processes are the cause of the large amount of holding memory in *Dead* process:

```
0x61EC066C mem_mgr: mem_mgr_chunk_t
0x61EC091C mem_mgr: mem_mgr_mempool_t
```

Workaround: Disable the **header-passing** command.

- CSCsj38829

Symptoms: When running double authentication crypto (ah encap and esp encap auth together) configurations and passing large packet data which requires fragmentation, errored packets can be observed.

Conditions: This symptom has been observed only on routers with AIM-VPN-PLUS AIM cards installed. Routers which support this AIM are the Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 routers.

Workaround: Do not use ESP and AH double authentication. You can use the **no crypto engine accel** command in the configuration to run encryption in the SW engine.

- CSCsj40156

Symptoms: Memory is leaking in case of radius-proxy users.

Conditions: This symptom is seen when a rad-proxy host object is already present in the SSG box, and it receives the access-request. The accounting starts from the proxy client, which is sent to the AAA server and AAA replies with an access-accept.

Workaround: There is no workaround.

- CSCsj46178

Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router either in global MGCP configuration or MGCP profile.

Workaround: Do not configure “endpoint naming t3”. Use t1 endpoint naming instead.

- CSCsj49255

Symptoms: If there is an ACL and DSCP being used for packet matching on class- map, only the first packet descriptor will get a match, and everything else will not. If DSCP is removed, the packet matching works again.

Conditions: This symptom is observed on a Cisco 7200 with ACL and DSCP with match all option.

Workaround: There is no workaround.

- CSCsj50773

Symptoms: Performing the **snmpwalk** on the ipRouteTable MIB may cause high CPU and reloads.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

Workaround: Create a view that excludes the ipRouteTable:

```
snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude
snmp-server view cutdown internet included
snmp-server community <comm> view cutdown RO
```

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

- CSCsj58796

Symptoms: No ringback is generated in calls from VoIP to a PBX end using Cisco Multicast Manager (CMM).

Conditions: This symptom has been observed when a call is made from the VoIP side to the PBX side through an MGCP-controlled CMM.

PBX <-----GW (CMM or Cisco 2620XM) <----CCM <----IP Phone

Workaround: Use a Cisco 2620XM router in place of CMM.

- CSCsj58969

Symptoms: Executing the **show port modem calltracker** command on a Cisco AS5400XM can cause bus error crash.

Conditions: This symptom occurs on a Cisco AS5400XM with multiple calls being made and terminated when running Cisco IOS Release 12.4(13a).

Workaround: There is no workaround.

- CSCsj63916

Symptoms: All DATA analog dialout calls are setting Bearer Capability to 0x8090 instead of 0x0890A3 (indicating the x-Law) where the A3 suffix is for A-law.

Conditions: This symptom has been observed on a Cisco AS5xxx router that is running Cisco IOS software later than Cisco IOS Release 12.4(7e) and having to make outgoing DATA calls.

Workaround: Change to Cisco IOS Release 12.4(7e).

- CSCsj64230

Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

Workaround: There is no workaround.

- CSCsj66692

Symptoms: Data corruption copy error tracebacks are seen on the console or output from the **show logging** command:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x41224EFC, -
Traceback= 0x4153A7D0 0x4155BA0C 0x4157FAF0 0x41224EFC 0x41DDC0A8 0x41DDC198
0x41DC6D84 0x41DF3B0C 0x41DC506C 0x41DCE5A4 0x41D91AF8 0x41D90F88 0x41D9BEFC
0x41D9C0C0 0x41DAEA68
```

Conditions: Refer to CSCsj44081 for more information.

Workaround: There is no workaround.

- CSCsj72647

Symptoms: On a Cisco IOS voice gateway, the **show call active voice brief** command output on the IP leg shows rx counters stay at 0 for 46 seconds.

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(7e).

Workaround: There is no workaround.

- CSCsj95947

Symptoms: The following message is seen on the router:

```
*Aug 6 16:34:47.188: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC=
0x8005EC50, -Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50
0x800651E4 0x800652A8 0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0 0x809E42D4
0x80A0854C 0x800DB8C0 0x800DEE48
```

Conditions: The conditions under which this symptom occurs are not known at this time.

Workaround: There is no workaround.

- CSCsj96577

Symptoms: A Cisco AS5400HPX crashes due to a bus error as indicated by show version “System returned to ROM by bus error at PC 0x61728370, address 0xB0D0B45”.

Just before the crash the following error message is seen:

```
%SYS-2-NOTQ: unqueue didn't find 674D6D40 in queue 3C -Process= "MGCP
Application", ipl= 0, pid= 170
```

Conditions: This symptom is observed on a Cisco AS5400HPX.

Workaround: There is no workaround.

- CSCsj97045

Symptoms: While running a Cisco IOS Release 12.4 Mainline release, a Cisco router may crash with a bus error. The error displayed will be similar to:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC =
0x605AFF94
```

Conditions: This symptom has been observed only if gateway is configured for Voice over IP (VoIP).

Workaround: There is no workaround.

- CSCsk00177

Symptoms: GRE traffic needs to be specifically allowed in the outside interface terminating DMVPN IPsec protected traffic.

Conditions: This symptom is observed on a DMVPN tunnel interface with tunnel protection Upset, with CEF or fasts witching.

Workaround:

- use process switching.
- allow the GRE traffic.

- CSCsk04970

Symptoms: There is a memory leak and fragmentation in *Dead* process due to MallocLite. After disabling mallocite, it will be seen as memory allocated to the “Virtual Exec” process in the **show memory allocating-process** [total] command output.

Conditions: The leak occurs whenever the **show vpdn session [l2tp] [all] username *username*** command is used, and there are many non-matching entries. Memory will be leaked proportional to the number of non-matching usernames (approximately 170 bytes per non-match).

Workaround: Avoid using the **show vpdn session [l2tp] [all] username *username*** command.

- CSCsk09651

Symptoms: A router crashes while a service policy is being attached, detached, or modified across a virtual template under traffic.

Conditions: This symptom is observed on a Cisco 7200 or Cisco 7301 router that is configured with MLPPP over FR on channelized interfaces.

Workaround: There is no workaround.

- CSCsk10985

Symptoms: IMA group interface does not come up after the reload.

Conditions: This symptom is observed on a Cisco 2811 router with ATM interface that is using VWIC2-2MFT-T1/E1 connected to MGX AUSUM card.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the IMA interface.

- CSCsk19661

Symptoms: In a Cisco 7500 HA router in RPR+ Mode when configuring and unconfiguring channel groups under an E1 controller, the router reports the following:

```
*Aug 22 17:58:34.970: %HA-2-IPC_ERROR: Failed to open peer port. timeout *Aug
22 17:58:34.974: %HA-3-SYNC_ERROR: CCB sync failed for slot: 1 *Aug 22
17:58:34.974: %HA-5-SYNC_RETRY: Reloading standby and retrying sync operation
(retry 1).
```

and the standby RSP is reloaded.

Conditions: This symptom is observed when configuring and unconfiguring channel groups under an E1 controller.

Workaround: There is no workaround.

- CSCsk25651

Symptoms: With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM)/CallManager and utilizing SRST functionality, when the IP phones are registered to the SRST router, the message-waiting indication (MWI) states may be incorrect.

Conditions: When a phone registers to a Cisco SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come, first-served fashion. The MWI state, however, is remembered from the previous registration that used that ephone-dn number so the MWI status could be incorrect.

Workaround: Configure both the SRST router and the CUE to use SUBSCRIBE/NOTIFY MWI method.

- CSCsk26774

Symptoms: Native VLAN information is not included in CDP packets going out ports of an EtherSwitch (ESW) module in Cisco 28xx and Cisco 38xx routers. All the platforms using switchports (of any kind built-in/NM/WIC/HWIC) have this issue: Cisco 8xx, Cisco 17xx, Cisco 18xx, Cisco 26xx, Cisco 36xx, Cisco 37xx, Cisco 28xx, and Cisco 38xx.

Conditions: This symptom causes Cisco IP phone models 7961, 7941 and 7970 that are running SCCP firmware to fail to forward traffic coming from a PC connected at the back of the phone.

Workaround: Enable the “Voice VLAN Access” setting on the phone.

- CSCsk36559

Symptoms: When one of the T1 or E1 controller NM-HDV2 goes down, the voice calls in the other controller are dropped.

This condition relates to interface x/0 x/0/0 (for example, 4/0 causes 4/0/0 to go down).

Conditions: This problem could happen in the MGCP PRI backhauled setup with NM- HDV2.

Workaround: There is no workaround.

- CSCsk60020

The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml>.

- CSCsk73104

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

- CSCsk88637

Symptoms: OAM cells are not generated when a new ATM subinterface and PVC is configured. Check subinterface and PVC status and enable the **debug atm oam interface atm/x.xxx** command. Subinterface will be up/up. PVC will be down, and no debug output will be seen.

Conditions: This symptom has been seen in various Cisco IOS 12.4 images.

Workaround: Perform **shut/no shut** commands on ATM subinterface.

- CSCsk97384

Symptoms: Abnormally large FreshTime value appears in IVR HTTP client cache entry.

Conditions: This symptom is observed when a VXML voice browser downloads a file from an HTTP server. If the file was modified very recently, the FreshTime for that file may show up with a very large value.

Workaround: There is no workaround.

- CSCsl14635

Symptoms: T38 negotiation is failing for the incoming UPDATE request having a T38 offer.

Conditions: This symptom occurs when the Voice gateway is running Cisco IOS Release 12.4(15)T and processing incoming Session Initiation Protocol (SIP) calls. When the SIP call is active and an UPDATE request is received which contains T38 offer, the UPDAE request is rejected. The switchover from voice to Fax fails.

Workaround: Fax over T38 works fine when midcall INVITE is used for T38 negotiation.

TCP/IP Host-Mode Services

- CSCsh92986

Symptoms: The latency for the **RSH** command could increase when they are flowing through an FWSM module.

Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3 which is not affected by this extra delay issue.

Wide-Area Networking

- CSCsh75479

Symptoms: A platform that is configured for ISDN may crash because of a bus error when you shut down an ISDN interface.

Conditions: This symptom is observed on a Cisco platform when traffic is being processed on the interface while you shut down the interface.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(13d)

Cisco IOS Release 12.4(13d) is a rebuild release for Cisco IOS Release 12.4(13). The caveats in this section are resolved in Cisco IOS Release 12.4(13d) but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCsi56413

Symptoms: The output may be stuck on a POS interface that is configured for Frame Relay encapsulation. When this situation occurs, the output queue is not emptied, and LMI remains down.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(12) or later. This happens only with very specific hardware configurations including NPE-G1 and PA-POS-OC3SMI. The issue observed when aforementioned Port Adapter is located at slot 4 and not seen with other hardware configurations.

Workaround: Place POS PA in other slot(s). PA location reconfiguration in chassis should fix the problem.

IP Routing Protocols

- CSCsg55591

Symptoms: When there are link flaps in the network, various PEs received the following error message:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
155:14344:10.150.3.22/32 from 10.2.2.1
```

Or, local label is not programmed into forwarding table for a sourced BGP VPNv4 network.

Conditions: This symptom occurs when an iBGP path for a VPNv4 BGP network is present. A sourced path for the same RD and prefix is brought up after.

Workarounds:

- Remove the iBGP path. If the sourced path comes up first, then the problem will not occur.
- Use different RDs with the different PEs. If the RD+prefix does not match exactly between the iBGP path and the sourced path, the problem will not occur.

ISO CLNS

- CSCsi57971

Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database in a local router.

Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsj72039

Symptoms: In ISIS, the prefix of a serial interface configured with PPP and passive interface in ISIS will not be part of the ISIS database. This problem can also be seen when the interface is configured as HDLC in place of PPP.

Conditions: This problem is seen with Cisco IOS Release 12.2(18)SXF6 and other releases.

Workaround: See the following workarounds:

- remove the **passive-interface** command and re-configure it.
- enter the **clear isis *** command.
- use any other command that would trigger the ISIS local database generation.

Miscellaneous

- CSCse64750

Symptoms: “%VPA-3-TSBUSY:VPA” and other error messages may be generated intermittently, and calls may fail.

Conditions: This symptom is observed on a Cisco 7206VRX that is configured with multiple VXC voice port adaptors.

Workaround: There is no workaround.

- CSCsg84975

Symptoms: MGCP NAS calls are dropped.

Conditions: This problem is seen when there are heavy E1 flaps.

Workaround: There is no workaround.

- CSCsi11996

Symptoms: The following error message is displayed on a Cisco AS5850 router every hour:

```
%HA_CLIENT-3-NO_CF_BUFFER: The MARVEL CRYPTO HA client failed to
get a buffer (len=1120) from CF (rc=1); checkpointing failed -Traceback=
0x201C9FBC
0x217C1B58 0x217C2068 0x21BBD32C 0x21BBDFD0 0x21BBE180 0x21DCF368 0x21DCF5C4
```

Conditions: This symptom has been observed on a Cisco AS5850 gateway running crypto images (c5850tb-k9p9-mz) in RPR+ mode.

Workaround: There is no workaround.

- CSCsi55964

Symptoms: After a gateway receives a high number of calls, calls may not go through intermittently.

Conditions: This symptom is observed on a Cisco 3800 series that functions as a gateway and that is configured for E1R2 signaling. The symptom occurs when the gateway sends a “clear forward” forward to the PSTN before the PSTN sends a “B1” message.

Workaround: There is no workaround.

- CSCsi57197

Symptoms: The T.37 Fax Offramp process may leak small amounts of memory.

Conditions: This symptom is observed on a Cisco router when the fax call on the PSTN side hangs up before the call completion.

Workaround: There is no workaround.

- CSCsi59685

Symptoms: One-way audio may occur and DTMF digits may not function.

Conditions: This symptom is observed on a Cisco gateway such as a Cisco AS5400 after a SIP transfer has occurred.

Workaround: Enter the **no voice-fastpath disable** command to resolve the one-way audio issue. There is no workaround for the DTMF issue.

- CSCsi64450

Symptoms: Many time out errors and many retries without any other IPC errors will be seen.

Conditions: This symptom is observed on a Cisco AS5850 platform.

Workaround. There is no workaround.

- CSCsi84017

Symptoms: When you reload a Cisco 2600 series, the router may hang.

Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCsj04563

Symptoms: SSG memory is leaking in Cisco IOS Release 12.4(13b).

Conditions: This symptom occurs when the RADIUS proxy feature is used. Leaking could be triggered on the following call flow scenario:

1. HostObject (HO) with MSID1, ip-address IP1 and username user1@cisco.com is logged on.
2. PDSN sends an acct-stop with MSID1 with session-continue attribute set to TRUE. When this is received, SSG will start a hand-off timer. Note that SSG will not delete the HO at this time.
3. Hand-off timer expires. HO is deleted.
4. SSG now receives an acct-start with MSID1 and username user1@cisco.com.
5. a) SSG will treat this as an auto-domain user, even though auto-domain is not configured on SSG. b) SSG will try to get the profile by extracting the domain name from the structured username and sending an access-req to AAA with username as the domain name. c) Since AAA server does not have the cisco.com profile, it sends an access-reject to SSG.
6. No HostObject is created.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsi91665

Symptoms: H.323 calls intermittently disconnect.

For each new call the H.323 GW will generate a TCP Port to be used for call setup. Intermittently the GW will generate a TCP Port that is being used for an established connection. When the GW initiates the three way handshake for the new call, it receives a response with an unexpected ACK sequence number. The GW will then send a TCP RST causing the currently established TCP connection/call to be torn down.

Conditions: This problem is observed in both Cystic IOS Release 12.4(13a) and Release 12.4(13b).

Workaround: There is no workaround.

Wide-Area Networking

- CSCsg89222

Symptoms: A PPP session that is initiated from a client may not be forwarded. to an LNS.

Conditions: This symptom is observed on a Cisco router after the PPP session has been established.

Workaround: Enter the **vpdn source-ip** global configuration command.

- CSCsh06841

Symptoms: A router may crash while establishing a PPP session.

Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsi74960

Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

Workaround: There is no workaround.

- CSCsi95921

Symptoms: When dial-peer “stat” changes to down, no calls can be made.

Conditions: This problem happens intermittently and does not seem to be related to any of the ISDN interface states.

Workaround: There is no workaround.

- CSCsj45426

Symptoms: Cisco AS5850 feature boards crash.

Conditions: This symptom occurs when giving the **no pri-group timeslots** command.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(13c)

Cisco IOS Release 12.4(13c) is a rebuild release for Cisco IOS Release 12.4(13). The caveats in this section are resolved in Cisco IOS Release 12.4(13c) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCsh51559

Symptoms: The following error message may be generated on a router that is configured for VPN or VPNv4:

For VPN:

```
ALIGN-3-SPURIOUS: Spurious memory access made at bgp_vpn_afmodify_walk
```

For VPNv4:

```
ALIGN-3-SPURIOUS: Spurious memory access made at bgp_vpnv4_afmodify_walk
```

Conditions: This symptom is observed on a Cisco router that is configured for BGP and IPv4 in a VRF address-family configuration and that imports routes from a VRF.

Workaround: There is no workaround. However, the error message is of a cosmetic nature and can be ignored.

- CSCsi62559

Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 12.2(18) and later.

Workaround: Use ACLs to block invalid IP Control packets from reaching the control plane.

- CSCsi84089

Symptoms: A router crashes by bus error a few seconds after OSPF adjacencies go up.

Conditions: This symptom has been observed on an ISR configured with OSPF running Cisco IOS Release 12.0S, Release 12.2S, Release 12.2SX, Release 12.2SRA, Release 12.2SRB or Release 12.4 images, but not in Release 12.2SRC or Release 12.3 images.

Workaround: Add area 0 in the OSPF VRF processes, or the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

Workaround: There is no workaround.

Miscellaneous

- CSCin30349

Symptoms: Interface flaps on an ATM IMA port adapter may cause the router to reload.

Conditions: This symptom has been observed when using an PA-A3-8T1IMA/PA-A3- 8E1IMA port adapter on Cisco 7xxx series router platforms. Flaps must be observed or the **shutdown** and **no shutdown** commands must be performed on an applicable interface. However, this symptom is a rare condition, and will not necessarily occur with every flap. This symptom can occur with or without traffic.

Workaround: There is no workaround.

- CSCsg70474

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsg99814

Symptoms: On a Cisco IOS router configured with GRE over IPSec or Virtual Tunnel Interface (VTI) configuration, this Access Control List (ACL) is bypassed if there is an ACL on the tunnel interface.

Conditions: This symptom occurs when there is another ACL configured on the outbound physical interface where the IPSec tunnel is terminated.

Workaround: Apply the ACL outbound on the protected LAN interface instead of the tunnel interface.

- CSCsh44798

Symptoms: An MGCP endpoint may become stuck and generate the following error message:

400 previous message in progress

Conditions: This symptom is observed when a call agent sends a CRCX message, either before receiving the acknowledgement for the previous DLCX message from the gateway or before acknowledging the previous DLCX message from the gateway.

Workaround: There is no workaround.

- CSCsh62737

Symptoms: On a Cisco router, the **fair-queue** command may be added to a multilink interface after reloading the router.

Before the reload:

```
interface Multilink4192
 ip address 10.1.1.1 255.255.255.252
 ppp multilink
 ppp multilink group 4192
 service-policy output 6144-VOIP
```

During the reload:

```
I/f Multilink4192 class VoIP-RTP requested bandwidth 1200 (kbps), available
only 45 (kbps)
```

After the reload:

```
interface Multilink4192
 ip address 10.10.10.1 255.255.255.252
 fair-queue 64 16 256
 ppp multilink
 ppp multilink group 4192
end
```

Conditions: This symptom has been observed on a Cisco 3845 router with 4 WIC-1DSU-T1-V2 running Cisco IOS interim Release 12.4(12.15) when multilink interface has a service-policy applied before reloading.

Workaround: Use the following procedure:

1. Remove the **fair-queue 64 256 256** command from the interface Multilink4192 and reapply the policy.
2. Downgrade to a version of Cisco IOS software before Cisco IOS Release 12.4(10), Release 12.4(8c), or Release 12.4(7d).
3. Change from absolute value of the **bandwidth** or **priority** commands to percentage values such as the **bandwidth percent** or **priority percent** commands like this:

```
policy-map 6144-VOIP
 class VoIP-RTP
  priority percent 33
 class VoIP-Control
  bandwidth percent 6
 class class-default
  fair-queue
  random-detect
```

- CSCsh70638

Symptoms: During system bootup or bursty traffic, the following error messages might be seen:

```
00:20:16: %ALIGN-SP-STDBY-3-SPURIOUS: Spurious memory access made at
0x72AB2370 reading 0xB8
00:20:16: %ALIGN-SP-STDBY-3-TRACE_SO: -Traceback= (s72033-
adventerprise9_wan_dbg-0-dso-bn.so+0x1AE370) ([42:0]+0x1AE47C) ([31:-3]3-dso-
b+0x220994) ([41:0]+0x220FB8) ([41:0]+0x221A90) ([41:0]+0x22214C) ([41:0]
```


+0x222D6C) ([41:0]+0x2233CC)

Conditions: This symptom has been observed with bursty IPC traffic during system booting up or switching over, typically with heavy configuration data exchanges.

Workaround: There is no workaround.

- CSCsh75827

Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the “J” Service-Info attribute), has logged out from the SESM, and then renews its IP address.

Workaround: There is no workaround.

- CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

- CSCsi27540

Symptoms: A VSI session can become stuck in the “RESYNC_UNDERWAY” state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

Workaround: There is no workaround.

- CSCsi67763

The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

<http://www.kb.cert.org/vuls/id/739224>

By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml>

- CSCsi78118

Symptoms: Traceback can be seen at “iphc_decompress”.

Conditions: This symptom has been observed in Cisco IOS interim Release 12.4 (13.13)T1.

Workaround: There is no workaround.

- CSCsi85641

Symptoms: The reverse-route remote-peer option does not correctly forward packets.

Conditions: CEF is enabled and the **reverse-route remote-peer** command is used. The **debug ip cef drops** command typically shows:

CEF-Drop: Stalled adjacency for remote-physical-ip-addr on Ethernet1/0 for destination remote-protected-ip-addr CEF-Drop: Packet for remote-protected-ip-addr -- encapsulation

Workaround: Disable CEF, or add a next hop to the reverse-route, such as with the **reverse-route remote-peer A.B.C.D** command.

- CSCsi99217

Symptoms: When 6000 L2TP sessions are disconnected, a Cisco IOS LNS router is stuck on High CPU Utilization (99% or 100%) with PPP IP Route process for 5 minutes.

Conditions: This symptom has been observed under stress test conditions (thousands sessions are disconnected at once) with no traffic and using Cisco IOS Release 12.4(13). This symptom has not been observed on earlier releases.

Workaround: There is no workaround.

Wide-Area Networking

- CSCsj10593

Symptoms: The trunking gateway (TGW) crashes when checked for gateway interconnect functionality for SETUP messages with all PRI switch types from User to NT side.

Conditions: This symptom has been observed with Cisco IOS interim Release 12.4 (15.6). This symptom occurs when the **isdn test call interface Serial1:23 22222** command is entered at the Call Starter and with Switch Types:

OGW: primary-ni

TGW: primary-dms100.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(13b)

Cisco IOS Release 12.4(13b) is a rebuild release for Cisco IOS Release 12.4(13). The caveats in this section are resolved in Cisco IOS Release 12.4(13b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeb20967

Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S, 12.1(14)E4, or 12.2 S when the following sequence of events occurs:

1. A packet is switched via Cisco Express Forwarding (CEF).
2. The egress interface has queueing/shaping configured.
3. The egress interface is congested, causing the packet to be placed into the hold queue.

Workaround: There is no workaround.

- CSCsh63542

Symptoms: The following SNMP error message and tracebacks are seen:

```
SEC 8:000049: Jan 31 22:25:00.760:
%SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe
regn with SNMP by driver having ifIndex 709 and ifDescr Tunnel0
-Traceback= 204128 204230 92DB90 92DF6C B2CF8C BBF368 BC00C8 1C4EFC 1C5524

1C60B8 1C655C 2EC5CC
```

Conditions: This symptom has been observed when new interfaces are added (or existing interfaces like tunnel come up) after bootup, or when new or existing interfaces come up after RPR+ switchover when running Cisco IOS Release 12.0(32)S6. Also, this symptom occurs if the **snmp ifindex persist** command is configured on the router.

Workaround: There is no workaround.

Further Problem Description: Though customer traffic is not affected, this symptom does impact the SNMP stats and other SNMP data for both the original and the new interface. Usually the message is from the standby RP, so once that standby RP becomes active, the data from SNMP polls of these interfaces would not be accurate.

IP Routing Protocols

- CSCsh02161

Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

Workaround: There is no workaround.

Miscellaneous

- CSCej42879

Symptoms: Traceback is seen while testing basic IPSec connection establishment and packet transmission between two peers in transmission mode and tunnel mode using Multilink Interface.

Conditions: This symptom has been observed on a Cisco 3845 Series router with Cisco IOS Release 12.4(5).

Workaround: There is no workaround.

- CSCek38201

Symptoms: A router may reload or display an alignment traceback when you enter the **show crypto socket** command.

Conditions: This symptom is observed on a Cisco router that has an OSPFv3 IPsecv6 configuration.

Workaround: There is no workaround. To prevent the symptom from occurring, do not enter the **show crypto socket** command in an OSPFv3 IPsecv6 configuration.

- CSCsd81407

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsg96319

Symptoms: Anyone can have unprivileged telnet access to a system without being authenticated, when a reverse SSH session is established with valid authentication credentials. This only affects reverse SSH sessions where a connection is made with the command **ssh -l userid:number ip-address** command.

Conditions: This symptom has been seen only when Reverse SSH Enhancement is used. This enhancement is documented at the following URL:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhant_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Workaround: Configure reverse SSH with the **ip ssh port portno rotary rotarygroup** command. This configuration is explained at the following URL:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newql

- CSCsh33430

Symptoms: A traceback may occur in an HSRP function and the platform may reload unexpectedly.

Conditions: This symptom is observed on a Cisco platform that has the HSRP Support for ICMP Redirects feature enabled and occurs when a learned HSRP group is removed after a resign message has been received.

Workaround: Disable the Support for ICMP Redirects feature by entering the **no standby redirects** global configuration command.

- CSCsh39318

Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

```
%MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of [dec] - VRF [chars]
```

Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

Workaround: There is no workaround.

- CSCsh55982

Symptoms: When you enter the **shutdown** command twice on an interface of a router, the interface on the peer shows that it is up, that is, the link is in the up/up state and the LED lights up.

Conditions: This symptom is observed on onboard Gigabit Ethernet interfaces of a Cisco 3800 series and Cisco AS5400 and does not occur on other platforms.

Workaround: Do not enter the **shutdown** command on an interface that is already shut down.

- CSCsh59375

Symptoms: The DHCP interface is not switched when the **ip dhcp smart-relay** command is enabled.

Conditions: This symptom has been observed with a Cisco 7200 router loaded with Cisco IOS interim Release 12.4(12.15a). The router is configured with an MPLS-VPN set up.

Workaround: There is no workaround.

- CSCsh92914

Symptoms: A router may unexpectedly reload when you attempt to open a reversed SSH connection by using the SSHv1 protocol.

Conditions: This condition is observed on a Cisco router that runs Cisco IOS Release 12.4.

Workaround: Force the SSH transport to be SSHv2 by entering the **ip ssh version 2** global configuration command.

- CSCsh94526

Symptoms: When an acct-stop message is received for a non-RADIUS proxy user (that is, a normal IP user), a router that is configured for SSG crashes.

Conditions: This symptom is observed when SSG is configured for RADIUS proxy mode and when the **ssg wlan reconnect** command is enabled.

Workaround: There is no workaround.

- CSCsh97579

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

- CSCsi04183

Symptoms: A router that is configured as an EasyVPN client is not able to auto connect to the EasyVPN server using its saved Xauth username/password.

Conditions: This symptom is observed when the router is powered-up or when the ISAKMP re-keying happens.

Workaround: Manually execute the **crypto ipsec client ezvpn xauth** command in the router console and enter the respective username/password.

- CSCsi04707

Symptoms: Configuring an AUX port for async interface through a non-slotted notation such as the **interface async 1** command or slotted notation such as the **interface async x/y/z** command may not be possible on a Cisco 2851.

Conditions: This symptom has been observed on a Cisco 2851 router with Cisco IOS Release 12.4(13). This symptom is not seen on Cisco IOS Release 12.4(3c) and earlier.

Workaround: There is no workaround.

- CSCsi27767

Symptoms: One-way audio may occur when a call is transferred or picked up after having been on hold.

Conditions: This symptom is observed intermittently on a Cisco Communication Media Module (CMM) for calls that are transcoded because of a transfer or being placed on hold and for which the RTP stream terminates on the CMM.

The symptom appears to occur because of a significant change in the sequence numbers and timestamp of the RTP packets while the same SSRC is kept. You can identify this situation with a packet capture of the RTP stream.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsi40766

Symptoms: H.323 calls on a Cisco IOS VoIP gateway may fail after the gateway has processed about 50,000 calls.

Conditions: This symptom is observed when H.323 uses TCP to transporting signaling messages. When the Cisco IOS gateway must generate a unique port for the local TCP session, this port is selected from a range of open ports. When the number of times that a unique TCP session is created for the same IP address on the gateway exceeds 54,500, further attempts to create a local TCP port fail and calls are not completed.

When the **debug ip tcp transaction** command is enabled on the gateway, the "TCP: Ran out of ports for network 0" debug output is generated when the symptom occurs.

Enabling debugs on a Cisco IOS gateway should always be done with caution to minimize impact to the performance of the router. As a minimum, ensure that logging to the console is changed from the default behavior of the debug level.

Workaround: Reload the Cisco IOS VoIP gateway. If this is not an option, there is no workaround.

Wide-Area Networking

- CSCsc28674

Symptoms: Using the **show call calltracker** command as well as requesting calltracker data via SNMP show incorrectly charged units.

Conditions: This symptom has been observed on a Cisco AS5350 gateway running Cisco IOS Release 12.3(16).

Workaround: There is no workaround.

- CSCse81069

Symptoms: Unconfiguring the **isdn service b_channel** command is not taking effect. The command is not removed from the running configuration.

Conditions: This symptom occurs when configuring the **isdn service b_channel** command to a state other than the default value of 0 on the ISDN D channel.

Workaround: To remove the command, shut down the T1/E1 controller first and then unconfigure the command under the D channel serial interface.

- CSCsh00185

Symptoms: A software forced-crash occurs with a memory corruption in the processor pool memory.

Conditions: This symptom is observed on a Cisco router that is configured for ISDN and that has an unusually long calling name with more than 70 characters in the received Facility IE.

Workaround: There is no workaround.

- CSCsh82513

Symptoms: The output of the **show isdn active** command may show disconnected calls.

Conditions: This symptom is observed on a Cisco router when analog modem calls are made after a normal ISDN digital call has been made.

Workaround: There is no workaround.

- CSCsh85902

Symptoms: For normal ISDN call and disconnecting the call, a DISCONNECT message will be issued. The contents of this DISCONNECT message will be replaced with the one that is explicitly configured. This configured message has an invalid facility component and hence the receiving side should send facility reject component which is not seen here (missing).

Conditions: This symptom happens with Cisco IOS Interim Release 12.4(12.15)T. This is happening only for Interface PRI and is seen for Cisco IOS Release 12.4 and Release 12.4T.

Workaround: There is no workaround.

- CSCsi21853

Symptoms: When you attempt to change the ISDN T306 timers, the changes are not accepted.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4.

Workaround: There is no workaround.

Further Problem Description: The ISDN T306 configuration updates the values of the ISDN T307 timers.

Resolved Caveats—Cisco IOS Release 12.4(13a)

Cisco IOS Release 12.4(13a) is a rebuild release for Cisco IOS Release 12.4(13). The caveats in this section are resolved in Cisco IOS Release 12.4(13a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsh76038

Symptoms: AAA enable authentication via a TACACS+ server fails.

Conditions: This symptom occurs when the **aaa authentication enable default group tacacs+** command or the **aaa authentication enable default group** command pointing towards a TACACS+ server group is configured.

Workaround: There are two possible workarounds.

1. On the TACACS+ server, configure a user named “\$enab{x}\$”, where {x} is the desired privilege level, such as using “\$enab15\$” for regular enable mode. This user password will be the enable password.
2. Change to a Cisco IOS release that does not yet include CSCin98780.

Further Problem Description: When using a RADIUS server, enable authentication is done by authenticating a user named “\$enab{x}\$”. When using a TACACS+ server, enable authentication is done by using the user’s actual username, which allows TACACS+ to define separate enable passwords for each user.

CSCin98780 erroneously caused the Cisco IOS software to authenticate “\$enab{x}\$” as a username for enable authentication for TACACS+ servers. This causes enable authentications in existing installations to fail, since TACACS+ server user databases do not normally contain a “\$enab{x}\$” user. This fix, CSCsh76038, corrects the issue, and any Cisco IOS release with this fix will transmit the user’s actual username again in any enable authentication request.

IP Routing Protocols

- CSCsh80678

Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

Conditions: This symptom is observed in Cisco IOS Release 12.3(22) when auto- summary is enabled for BGP.

Workaround: Use the **no auto-summary** command.

- CSCsh90153

Symptoms: Connectivity is lost through a router when traffic is processed twice by NAT.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(8a), that is configured for NAT and PBR, and that has a firewall feature enabled. Under certain conditions, traffic is processed twice by NAT when it does not need to be.

Workaround: Remove the firewall configuration from the router.

Further Problem Description: Syslogs and the output of the **show ip nat translation** command show that traffic that is processed twice by NAT does not traverse the router.

Miscellaneous

- CSCds25257

Symptoms: Gatekeeper Rejects new registration requests from CUCM or other H.323 endpoints with RRJ reason of duplicateAlias. Attempting to clear this stale registration fails with “No such local endpoint is registered, clear failed.” message.

Conditions: CUCM H.225 trunks register to a gatekeeper (GK) cluster. GK1 and GK2 are members of the GK cluster. CUCM registers first to GK1 then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

Once the H.225 trunk attempts to register with GK1, it gets rejected because the alternate registration is still present, and there is no way to clear it out.


```

10.9.20.3      34273 10.9.20.3      32853 SJC-LMPVA-GK-1      H323-GW A
ENDPOINT-ID: 450FC24400000000 VERSION: 5 AGE: 1618993 secs
SupportsAnnexE: FALSE
g_supp_protos: 0x00000050
H323-ID: SJC-LMPVA-Trunk_4

```

Workaround: Reset the gatekeeper with the **shutdown** command followed by the **no shutdown** command, or reboot the Cisco IOS GK.

- CSCsf28509

Symptoms: When you enter the **clear ip dhcp binding** command to clear DHCP bindings, the corresponding DHCP-initiated subscriber sessions are not cleared.

Conditions: This symptoms is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Enter the **clear ip subscriber** command to clear the subscriber sessions.

- CSCsg59326

Symptoms: When an ATM (cash machine, not the WAN technology) box is connected to a switch service module, there is significant packet loss.

Conditions: This symptom is observed on a Cisco 2800 series router.

Workaround: Change Ethernet speed to 10mbps on both ends.

- CSCsh22469

Symptom 1: On POTS-to-POTS calls between an originating analog voice-port over a PRI trunk, terminating on another voice-port, call attempts fail because the outgoing ISDN Q.931 SETUP has an incorrect Bearer Capability:

```

Dec  7 12:54:12.596: ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16
is 0x0 0x0, Calling num 123456789
Dec  7 12:54:12.596: ISDN Se0/0/0:15 Q931: Applying typeplan for sw-type 0x16
is 0x0 0x0, Called num 987654321
Dec  7 12:54:12.596: ISDN Se0/0/0:15 Q931: TX -> SETUP pd = 8  callref =
0x497A

    Sending Complete
    Bearer Capability i = 0x9090
        Standard = CCITT
        Transfer Capability = 3.1kHz Audio
        Transfer Mode = Circuit
        Transfer Rate = 64 kbit/s
    Channel ID i = 0xA98383
        Exclusive, Channel 3
    Progress Ind i = 0x8183 - Origination address is non-ISDN
    Calling Party Number i = 0x0080, '123456789'
        Plan:Unknown, Type:Unknown
    Called Party Number i = 0x80, '987654321'
        Plan:Unknown, Type:Unknown
Dec  7 12:54:12.660: ISDN Se0/0/0:15 Q931: RX <- RELEASE_COMP pd = 8
callref
= 0xC97A

```

```
Cause i = 0x82C131903980 - Bearer capability not implemented
Display i = 'BEARER CABABILITY NOT IMPLEMENTED'
```

The correct Bearer Capability for the E1 PRI should be 0x9090A3 for G.711 A-law. For a T1 PRI the correct Bearer Capability would be 0x9090A2 for G.711 u-law.

Symptom 2: The same issue with the outgoing Q.931 SETUP having an incorrect Bearer Capability is observed on VoIP-to-POTS calls when the PRI voice-port has the **bearer-cap speech** command configured.

Conditions: This behavior is observed on a Cisco IOS Voice Gateway where a voice call is made originating at an analog POTS interface, and going over a PRI trunk. If the originating voice-port is a digital POTS trunk or an EFXS (CME/SRST ephone) POTS interface, there is no corruption of the bearer-cap in the outgoing Q.931 SETUP.

The problem may also be observed on regular VoIP-to-POTS call scenarios if the **bearer-cap speech** command is configured on the PRI voice- port.

There are no known scenarios where there is a bearer-cap problem for an incoming call on the PRI voice-port.

The Voice Gateway is installed with Cisco IOS specified by or implied by the “First Fixed-in” field of bug ID CSCsf20569 “Oct5_Present and encoding to be used in call setup request.”

Workaround: There is no workaround available other than to use an unaffected Cisco IOS release. Cisco IOS releases up to 12.4(12) and 12.4(11)T are unaffected by this defect.

Resolved Caveats—Cisco IOS Release 12.4(13)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(13). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(13). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCse67406

Symptoms: Locally destined traffic does not show up in the NetFlow cache and traffic that is dropped by an ACL is not accounted for on the RSP.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: There is no workaround.

- CSCsf12539

Symptoms: Tracebacks may be generated for all accounting messages.

Conditions: This symptom is observed on a Cisco router that is configured for AAA.

Workaround: There is no workaround.

- CSCsg48183

Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

- You reload the router.
- A switchover of the active RP occurs.
- You enter the **redundancy force-switchover main-cpu** command.

Workaround: There is no workaround.

- 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. Is this not an option, there is no workaround.

- CSCsh02125

Symptoms: A traceback is generated when you enter the **show snmp** command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: There is no workaround.

- CSCsh02375

Symptoms: The output of the **show controller cbus** command does not list details for any interfaces other than serial interfaces.

Conditions: This symptom is observed on the RPS of a Cisco 7500 series.

Workaround: There is no workaround.

- CSCsh44174

Symptoms: After a router has crashed, another crash may occur while the crashinfo is being generated, and a traceback with memory addresses is displayed.

Conditions: This symptom is observed on a Cisco router when, during the crash, the data in key memory locations is written to a crashinfo file on the bootflash device of the router.

Workaround: Specify an alternate storage device to store the crashinfo in the startup configuration, for example, by adding the following line to the startup configuration:

```
exception crashinfo disk0:
```

- CSCuk61422

Symptoms: CEF-switching does not function, and the output of the **show adjacency interface interface-number detail** command does not show any packets.

Conditions: This symptom is observed on a Cisco 7500 series that has an RSP when packets are switched to a multilink interface via CEF and when you enter the **show adjacency interface interface-number detail** for a multilink interface.

Workaround: There is no workaround.

IBM Connectivity

- CSCsg65485

Symptoms: A Cisco 7206VXR that is configured for Data-Link Switching (DLSw) may reload unexpectedly.

Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS interim Release 12.3(20.12).

Workaround: There is no workaround.

Interfaces and Bridging

- CSCek43732

Symptoms: All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for CBWFQ.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1. However, the symptom may be platform-independent.

Workaround: There is no workaround.

- CSCsg64182

Symptoms: A VIP may crash because of a bus error.

Conditions: This symptom is observed when a dot1q subinterface on the VIP is configured with a service policy.

Workaround: Remove the service policy.

- CSCsg75064

Symptoms: A Logical Link Control (LLC) device can connect to a SNASwitch port by using an HSRP standby MAC address on a different dot1q VLAN than the one that is defined.

Conditions: This symptom is observed when the SNASwitch port has a dot1q VLAN subinterface configured and when there are other dot1q subinterfaces configured that use HSRP and individual standby MAC addresses.

Workaround: Use ISL trunk VLAN subinterfaces, on which the symptom does not occur.

Further Problem Description: In the following example, a SNASw has a port that is defined in VLAN 56 so devices can connect to MAC address 0200.0000.0055. However, devices can also connect to the SNASw by using MAC address 0200.0000.0056:

```
interface FastEthernet0/0.55
 encapsulation dot1Q 55
 ip address
 standby 2 ip
 standby 2 mac-address 0200.0000.0055
!
interface FastEthernet0/0.56
 encapsulation dot1Q 56
 ip address
 standby 1 ip
```

```
standby 1 mac-address 0200.0000.0056
!
snasw port FAST0056 FastEthernet0/0.56 conntype len
```

- CSCsh16540

Symptoms: A router crashes when you enter the **encapsulation dot1q** *vlan-id* command.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(12.7) and that is configured for MPLS. However, the symptom is platform-independent.

Workaround: There is no workaround.

- CSCuk61108

Symptoms: Packets may become corrupted with a faulty VLAN tag when they are forwarded over an FE interface.

Conditions: This symptom is observed when the FE interface has subinterfaces that are configured for dot1q encapsulation.

Workaround: There is no workaround.

IP Routing Protocols

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>.

- CSCei29944

Symptoms: A CE router that has L2TP tunnels in an MPLS VPN environment with about 1000 VRFs may crash and generate the following error message:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x50766038
```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)S and that functions as a CE router when BGP neighbors are unconfigured via the **no neighbor** *ip-address* command while the **show ip bgp summary** command is entered from the Aux console. The symptom is not release-specific and may also affect other releases.

Workaround: There is no workaround.

- CSCek45564

Symptoms: A router crashes because of memory corruption when you bring up Gigabit Ethernet links and BGP neighbor adjacencies, and an error message is generated, indicating that a block overrun and rezone corruption have occurred.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series that are configured for BGP. However, the symptom is not platform-dependent.

Workaround: There is no workaround.

- CSCsc67367

Symptoms: The **set ip next-hop in-vrf** *vrf-name* command does not work in conjunction with import maps.

Conditions: This symptom is observed on a Cisco router that is configured for BGP.

Workaround: There is no workaround.

- CSCsc74229

Symptoms: A router may delete the VPNv4 prefixes from the BGP table, even though the counters in the output of the **show ip bgp** command may indicate that the VPNv4 prefixes are present in the BGP table. This situation may cause loss of VPN connectivity.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and that functions as a PE router.

Workaround: There is no workaround. When the symptom occurs, enter the **clear ip bgp *** command to restore proper operation of the router.

- CSCse97264

Symptoms: Two or more UDP NAT translations that relate to different requests may be assigned port numbers with the same inside global IP address.

Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.3(11)T9, Release 12.4, or Release 12.4T when more than one IP phone attempts to register through a router that is configured for NAT Overload.

Workaround: There is no workaround.

- CSCsf20947

Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsg29248

Symptoms: A stale LSA may be created when you enter the **summary-address not-advertise** command.

Conditions: This symptom is observed when a self-originated external LSA with the same address and a more specific mask already exists in the OSPF database. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf27810>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Clear the OSPF process.

- CSCsg43140

Symptoms: A router may crash during the boot process and return to ROMmon.

Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has VPNs configured.

Workaround: There is no workaround.

- CSCsg48509

Symptoms: The **match-in-vrf** keyword is missing from the **ip nat inside source** command, and the **ip nat inside source** command is not accepted at all in interface-configuration mode.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(11.6a) or interim Release 12.4(12.03)T but may also affect other routers.

Workaround: There is no workaround.

- CSCsg50321

Symptoms: A router may hang when you enter the **clear ip nat translation *** command.

Conditions: This symptom is observed on a Cisco 7500 series that has an RSP when you configure static NAT for an inside source address.

Workaround: There is no workaround.

- CSCsg52336

Symptoms: A router may crash when you remove an unused and unassigned VRF by entering the **no ip vrf vpn-name** command.

Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the Multi-VRF capability for OSPF routing configured along with other VRFs that are unused and unassigned.

Workaround: There is no workaround.

- CSCsg55209

Symptoms: When BGP updates are received, stale paths are not removed from the BGP table, causing the number of paths for a prefix to increase. When the number of BGP paths reaches the upper limit of 255 paths, the router resets.

Conditions: This symptom is observed on a Cisco router when the **neighbor soft-reconfiguration inbound** command is enabled for each BGP peer.

Workaround: Remove the **neighbor soft-reconfiguration inbound** command. A router that runs a Cisco IOS software image that has a route refresh capability, storing BGP updates is usually not necessary.

- CSCsg59699

Symptoms: The OSPFv3 cost on PortChannel interfaces that is calculated based on the interface bandwidth may not be correct.

Conditions: This symptom is observed on a Cisco router when OSPF functions in IPv6 router configuration mode and when the **auto-cost reference-bandwidth** command is enabled.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected PortChannel interface.

- CSCsg66635

Symptoms: The IGP metric may be missing from the TE database.

Conditions: This symptom is observed on a Cisco router when TE is configured on a subinterface and when you enter the **no shutdown** interface configuration command on the physical main interface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface on which TE is configured.

- CSCsg71344

Symptoms: On a router that is configured for SSM and that is connected to an upstream router via two interfaces, when one of the interfaces is shut down and brought up again, a PIM Join message is not sent.

Conditions: This symptom is observed on a Cisco router that is connected to an upstream router via an RPF interface. When the interface of the upstream router that connects to the RPF interface is shut down, the PIM Join message is sent via the other interface on the Cisco router. However, when the interface of the upstream router that connects to the RPF interface is brought up again, the PIM Join message is not sent again, preventing IPv6 multicast from functioning properly.

Workaround: There is no workaround.

- CSCsg84690

Symptoms: A default route with an incorrect mask may not be installed.

Conditions: This symptom is observed on a Cisco router that is configured for OSPF.

Workaround: There is no workaround.

- CSCsg84883

Symptoms: NAT configurations are not removed.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: There is no workaround.

- CSCsg94794

Symptoms: When VRF-aware NAT is configured with FTP, the data connection that is dynamically created may appear in the global routing space instead of in the matching VRF, causing the transfer to fail.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T and that is configured for VRF-aware NAT.

Workaround: There is no workaround.

Further Problem Description: In order for the fix for caveat CSCsg94794 to be complete, the fix for caveat CSCsh45022 is also required. For information about caveat CSCsh45022, see the Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh45022>.

- CSCsh19852

Symptoms: When an OSPF interface goes down, some Finite State Machine (FSM) events do not occur. For example, old network LSAs may not be removed by the Designate Router (DR).

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCek63900. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCek63900>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsh24066

Symptoms: A Cisco 7400 series or Cisco 7500 series with any ATM port adapter may crash when traffic is sent.

Conditions: This symptom is observed when the router is configured for Next Hop Resolution Protocol (NHRP).

Workaround: There is no workaround.

ISO CLNS

- CSCsg28497

Symptoms: An IS-IS adjacency may flap when an RP switchover occurs.

Conditions: This symptom is observed on a Cisco router that is configured for IS-IS Multi-Topology, IS-IS NSF Awareness, and IPv4 and IPv6 unicast.

Workaround: There is no workaround.

Miscellaneous

- CSCdv43124

Symptoms: A Cisco VIP4-80 with a PA-MC-STM-1SMI crashes when QoS is deployed and traffic is processed.

Conditions: This symptom is observed on a Cisco 7500 series when the VIP4-80 is connected to a CE router.

Workaround: Reload the Cisco VIP4-80. Doing so enables the router to reconnect to the CE router.

Further Problem Description: Replacing the Cisco VIP4-80 does not resolve the symptom.

- CSCed57504

Symptoms: A router that is configured with a virtual template may reload unexpectedly.

Conditions: This symptom is observed on a Cisco router on which a session that uses a virtual-template is terminated and occurs when the session is cleared from a DSL CPE router that is the peer router for the connection.

Workaround: There is no workaround.

- CSCed83434

Symptoms: On a line card, the VPN prefixes in one VRF may be attached to another VRF.

Conditions: This symptom is observed when more than one VRF is configured in nonalphabetical order and a when an RPR+ switchover occurs.

Workaround: After configuring VRFs, reload the router before a switchover can occur.

- CSCeh41598

Symptoms: When RIP is enabled and disabled successively 50 to 60 times in a row, the router reloads unexpectedly during the “RIP managed timer” process.

Conditions: This symptom is observed on a Cisco router that has 15,000 learned RIP prefixes. However, note that RIP does not properly scale beyond about 5000 routes on a high-end router.

Workaround: Do not enable and disable RIP successively 50 to 60 times in a row.

First Alternate Workaround: Limit the number of RIP prefixes to 5000 or less.

Second Alternate Workaround: Before RIP is disabled, for example through the **no router rip** command, remove the network entries under the **router rip** command.

- CSCek42751

Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

Workaround: Reboot the router once more.

- CSCek48251

Symptoms: When you enter the **redundancy switch-activity force** command on the active eRSC of a Cisco AS5850 while incoming VoIP H.323 calls and outgoing CAS calls are being processed, the standby eRSC does become the active eRSC and processes the calls but soon afterwards may crash at “csm_enter_idle_state.”

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(9)T and that functions in RPR+ mode. The symptom may also affect Release 12.4.

Workaround: There is no workaround.

Further Problem Description: The symptom does not occur when PRI calls are being processed.

- CSCek48471

Symptoms: A callback on an asynchronous interface may fail.

Conditions: This symptom is observed on a Cisco router that has the **modem autoconfigure discovery** command enabled.

Workaround: Remove the **modem autoconfigure discovery** command from the configuration.

- CSCek50380

Symptoms: A Cisco router may crash with an illegal opcode exception when you configure dot1q encapsulation on a subinterface.

Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.4, a rebuild of Release 12.4(4)T, or Release 12.4(9)T. Note that the symptom may be platform-independent. The symptom occurs under the following conditions:

- A policy map is configured on the router and more than 10 classes are specified in the policy rules.
- The **service-policy input** *policy-map-name* and **service-policy output** *policy-map-name* commands are configured on the main interface.

Workaround: First configure the subinterface for dot1q encapsulation. Then, enter the service-policy statements.

Important Note: If you apply the workaround, save the configuration, and then reload the router, the router will cycle continuously while booting the configuration. Do not save the configuration with the service policy applied.

- CSCek55486

Symptoms: The native Gigabit Ethernet (GE) interface on an NPE-G1 card may reset unexpectedly.

Conditions: This symptom is observed on a Cisco 7200 series when the underrun counter for the native GE interface increments continuously. You can verify the underrun counter in the output of the **show interfaces gigabitethernet slot/port** command.

Workaround: There is no workaround.

- CSCek55511

Symptoms: A Cisco AS5400HPX that is running Cisco IOS Release 12.3(11)T7 may crash with IO Memory corruption.

Conditions: The crash may occur when polling for ccrpCPVGEEntry, and resource pooling is enabled on the Gateway.

Workaround: Disable SNMP polling for ccrpCPVGEEntry.

- CSCek61276

Symptoms: IPv6 traffic stops.

Conditions: This symptom is observed on a Cisco router when you first disable and then re-enable IPv6 on an interface.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCek64432

Symptoms: A VoiceXML Gateway that has an ASR/TTS traffic load may crash.

Conditions: This symptom is observed on a Cisco router that functions as a VoiceXML Gateway with a high volume of VXML calls with ASR/TTS interactions.

Workaround: There is no workaround.

- CSCek64789

Symptoms: A router that is configured as a voice gateway may crash because of a bus error. Just before the crash occurs, messages of the following type may be generated:

```
%ALIGN-1-FATAL: Corrupted program counter
```

Conditions: This symptom is observed on a Cisco 2811 that is configured as a Cisco Multiservice IP-to-IP Gateway (IPIP GW). However, the symptom is not platform-dependent.

Workaround: There is no workaround.

- CSCek66164

Symptoms: A router may hang briefly and then may crash when you enter any command of the following form:

```
show ... | redirect rcp:....
```

Conditions: This symptom is observed when Remote Copy Protocol (RCP) is used as the transfer protocol.

Workaround: Use a transfer protocol other than RCP such as TFTP or FTP.

Further Problem Description: RCP requires delivery of the total file size to the remote host before it delivers the file itself. The output of a **show** command is not an actual file on the file system nor is it completely accumulated before the transmission occurs, so the total file size is simply not available in a manner that is compatible with RCP requirements.

- CSCin99554

Symptoms: A router hangs when you stop a core dump in progress by pressing the CTRL+SHIFT+6 keys.

Conditions: This symptom is observed only when you use RCP for a core dump.

Workaround: Do not use RCP for a core dump.

- CSCir00361

Symptoms: The E1 layer entries for a channelized E3 port adapter may be missing from the IF-MIB list, causing the absence of the corresponding DS1 layer Descriptor and Stack entries when an SNMP walk is performed.

Conditions: This symptom is observed on a Cisco router that functions in a very simple configuration in which a channelized E3 port adapter is configured with several E1 layers.

Workaround: There is no workaround.

- CSCsa80126

Symptoms: The SNMP IfIndex Persistence feature may not function as expected. The ifIndex table that is created when you enter the **snmp-server ifindex persist** command is not loaded when the router boots and the indexes of all interfaces are reassigned in a sequential order that depends on the interface number.

Conditions: This symptom is observed on a Cisco router when you first create a subinterface with a sequence number that is lower or in between the numbers of the existing interfaces and then you reload the router.

Workaround: There is no workaround.

- CSCsb15138

Symptoms: The following error messages may be generated on a gateway that functions in a configuration in which 80 channels are processed by a VXML Server, and the call may be dropped:

```
//-1//HTTTPC:/httpc_streaming_create: attempt to create a session with id 699 while
this id is in use //2144684/0BCEFB9AA28/VXML:/vxml_media_done:
CALL_ERROR; fail with vapp error 2, protocol_status_code=0
//2144684/0BCEFB9AA28/VXML:/vxml_media_done:
CALL_ERROR; *** error.badfetch.http.0 event is thrown
```

Conditions: This symptom is observed rather rarely on a Cisco AS5400 gateway when the HTTP client session IDs range from 1 to 2048 because of the socket limit per Cisco IOS process. The error messages are generated when the HTTP client attempts to create a new session with the same ID as an old session that is still in use. In this situation, only a benign warning message should be generated, and the call should be accepted. If an HTTP streaming session remains in use for a long time and the traffic load of the gateway is high, the symptom is more likely to occur.

Workaround: Configure an event handler as in the following example:

```
<catch event="error.badfetch.http.0">
<!-- Actual event handler goes in here -->
</catch>
```

If this is not an option, the symptom may be mitigated by disabling IVR streaming mode via the **ivr prompt streamed none** command.

- CSCsc71245

Symptoms: A router that is connected to several VPN clients may unexpectedly reload because of a CPUHOG condition in the crypto IKMP process followed by a watchdog timeout.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and occurs about every about 24 hours, which is equal to the IKE lifetime.

Workaround: There is no workaround.

- CSCsd52438

Symptoms: Frame Relay Traffic Shaping (FRTS) is not engaging properly, and voice traffic is not being protected when using the on-board T1 port from the NM-HDV2-T1/E1 module.

Conditions: This symptom occurs during negative testing of QoS features on a Cisco 3745 router that is running Cisco IOS Release 12.3(11)T9. When overdriving Default (BE) and Deterministic (AF11) queues, drops do not register in the Default queue. Also, voice quality is poor when call is placed over the circuit.

Workaround: Do not use the T1 port on-board the NM-HDV2-T1/E1 module.

Further Description: The problem seems unique to the NM-HDV2 modules

- CSCse31572

Symptoms: A router that is configured for DMVPN may reload because of a bus error.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T. The symptom could occur in Release 12.4.

Workaround: There is no workaround.

- CSCse53212

Symptoms: When a switchover occurs, a traceback may be generated on a router that is configured with a large number of PPPoE sessions, and the router may crash.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS and LDP and occurs only when the number of PPPoE sessions reaches beyond 30,000. However, the traceback (without a crash) may occur even for 500 PPPoE sessions.

Workaround: There is no workaround.

- CSCse80723

Symptoms: A Communication Media Module (CMM) may fail to come online after it has been reloaded, power-cycled, or crashed. The output of the **show test module** command for the CMM indicates that the loopback test on port 1 of the module has failed:

```
Loopback Status [Reported by Module 1] :
```

```
Ports 1  2  3  4  5
```

```
-----
```

```
F  N  N  N  .
```

Conditions: This symptom is observed on a Cisco Catalyst 6000 series that has a Supervisor Engine 2 that runs CatOS 8.5(5) software and a CMM that runs Cisco IOS Release 12.4.

Workaround: Enter the **clear cam dynamic** and reset the CMM once more.

- CSCse90464

Symptoms: When a router receives IP fragments that match an access control list (ACL), a spurious memory access may occur and the router may crash.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T, Release 12.4, or Release 12.4T when an extended ACL is configured and when the router receives IP fragments that match the ACL.

Workaround: If the Turbo ACL feature is an optional feature on the router, disable the Turbo ACL feature by entering the **no access-list compiled** command. If the Turbo ACL feature is not an optional feature on the router, that is, it is always enabled, there is no workaround. On the Cisco RPM-XF there is no workaround.

- CSCse99958

Symptoms: A Cisco router may fail to access a flash card after formatting it, and the following error message is generated:

```
*** Emulating mis-aligned load at 0x80000190
PC = 0x8001179c ... succeeded
```

Conditions: The symptom is observed on a Cisco 7200 series, Cisco 7301, and Cisco 7500 series that run Cisco IOS Release 12.4(10) or Release 12.4(12) and occurs only when a flash card is accessed from the ROMmon prompt.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(8a) or an earlier release.

- CSCsf25712

Symptoms: A line card such as a SIP-200 may crash when the line card on the other side or SPAs in the line card on the other side are reloaded.

Conditions: This symptom is observed on a router that has a highly scaled configuration (for example, a configuration that is used for mobile users) with priority traffic and non-priority traffic running at line rate.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because of memory corruption.

- CSCsf30618

Symptoms: A DHCP route is unexpectedly removed for an unnumbered DHCP binding.

Conditions: This symptom is observed when a DHCP address is renewed.

Workaround: There is no workaround. However, during the next DHCP address renewal, the DHCP route is added back.

- CSCsf95938

Symptoms: A memory leak occurs in the middle buffers after all onboard DSPRM pools are depleted.

Conditions: This symptom is observed on a Cisco 3800 series router that runs Cisco IOS Release 12.4(7b) with support for CVP survivability.

Workaround: There is no workaround.

- CSCsg00673

Symptoms: When you enter the **show memory statistics** command and query the same data via SNMP, the values do not match for transient memory.

Conditions: This symptom is observed on a Cisco router that is queried via SNMP.

Workaround: There is no workaround.

- CSCsg05350

Symptoms: A Cisco platform crashes due to a chunk memory leak and generates the following error messages and tracebacks:

```
%DSMP-3-INTERNAL: Internal Error : NO MEMORY
-Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
0x6127F6BC
%DSMP-3-INTERNAL: Internal Error : NO MEMORY
-Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
0x6127F6BC
%MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a reload due to Fragmented
processor_memory, Free processor_memory = 10402472 bytes, Largest processor_memory
block = 522632 bytes
```

Conditions: This symptom is observed on a Cisco AS5850 when there is a chunk memory leak. However, the symptom is platform-independent and relates to the Distributed Stream Media Processor (DSMP).

Workaround: There is no workaround.

- CSCsg08395

Symptoms: When one of the controllers of a VWIC-2MFT-E1 Voice/WAN interface card that is connected back-to-back to another router is shut down, ISDN L2 may go down on the second E1 controller of the VWIC-2MFT-E1.

Conditions: This symptom is observed on a Cisco 3725 that runs Cisco IOS interim Release 12.4(11.1).

Workaround: There is no workaround.

- CSCsg09208

Symptoms: A router may reload unexpectedly when you apply an IPS policy to an interface.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(10) or a later release and that uses Signature Definition File (SDF) version 6 files.

Workaround: There is no workaround.

- CSCsg11750

Symptoms: Unexpected call failures and slow but steady increases in overall memory utilization occur, and the router crashes because of memory errors or memory depletion.

Conditions: This symptom is observed on a Cisco PSTN gateway that has an NM-HDV2 network module on which the DSPs terminate PRI trunks and run DSPFarm media resources such as transcoders and conference resources. Calls are routed to and from Cisco Unified CallManager call processing servers.

Workaround: There is no workaround.

- CSCsg21401

Symptoms: Calls may fail on a gatekeeper. When this situation occurs, you may not be able to Telnet or ping to the gatekeeper, and the logs of the gatekeeper contain several error messages with tracebacks that indicate “bad id in id_get”. In addition, gateways may also unregister from the gatekeeper.

The following error message and traceback are generated when the symptom occurs:

```
%IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x6445D720)
-Traceback= 0x6114DA04 0x622C7944 0x610F767C 0x610F8228 0x610F8138 0x6110C854
0x6110CBB8 0x60074F1C 0x60063D74 0x60040B94 0x60052A84 0x6002637C 0x60028AB0
```

Symptoms: This symptom is observed on a Cisco platform that functions as a gatekeeper in an H.323 environment.

Workaround: There is no workaround.

- CSCsg28628

Symptoms: NAS pkg asynchronous calls fail after a redundancy switchover has occurred, and the following error message is generated:

Modems unavailable

Conditions: This symptom is observed on a Cisco AS5850 that functions in RPR+ mode. This situation may impact service.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **redundancy switchover** command a couple of times to restore the Cisco AS5850 to normal operation.

- CSCsg30880

Symptoms: After a router is booted or reloaded, a PVC bundle configuration that is established under an IMA interface is lost.

Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.3(11)T7 or Release 12.3(14)T7 and that has the **service-policy output** command enabled on the PVC bundle. The symptom may also affect Release 12.4 and Release 12.4T.

Workaround: Disable the **service-policy output** command on the PVC bundle.

- CSCsg36982

Symptoms: A static route is not removed when you enter the **clear ip dhcp binding** command.

Conditions: This symptom is observed on a Cisco router when the DHCP binding and route are loaded from a database agent.

Workaround: Do not use a database agent for the restoration of a binding and router.

- CSCsg37423

Symptoms: The output of the **show l2tun session l2tp** command does not include interface information.

Conditions: This symptom is observed on a Cisco router that is configured for Xconnect.

Workaround: There is no workaround.

- CSCsg39287

Symptoms: A memory leak and fragmentation may occur on a terminating H.323 gateway upon receipt of an H.225 Notify message, and the gateway may crash.

Conditions: This symptom is observed on a Cisco AS5400 that has been processing calls for a couple of days.

Workaround: There is no workaround. There would be a workaround if you could prevent the originating device from sending Notify messages. However, this is not an option in a typical Cisco CallManager IP Telephony (IPT) deployment.

- CSCsg40482

Symptoms: ISDN L2 may remain in the "TEL_ASSIGNED" state.

Conditions: This symptom is observed on a Cisco router after you have performed a hard OIR of a PA-MC-4T1 port adapter.

Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload the router.

- CSCsg40567

Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

Workaround: Disable the **ip http secure server** command.

- CSCsg42246

Symptoms: High CPU use may occur in the “IP Background” process, and the router may reload unexpectedly.

Conditions: This symptom is observed on a Cisco router that is configured for RIP and that receives a RIP host route that is subsequently replaced by a route that is dynamically assigned to an interface. For example, this situation may occur on a PPP interface that has the **ip address negotiated** command enabled.

Workaround: Use a route map to block the advertised route.

- CSCsg50187

Symptoms: CEF-switching does not function, and the output of the **show adjacency interface interface-number detail** command does not show any packets.

Conditions: This symptom is observed on a Cisco router when packets are switched to a multilink interface via CEF and when you enter the **show adjacency interface interface-number detail** for a multilink interface.

Workaround: There is no workaround.

- CSCsg50190

Symptoms: When you enter the **erase /all nvram:** command, the command is rejected and a “% Unrecognized command” error message is generated.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(11.3) or a later release or interim Release 12.4(11.3)T or a later release.

Workaround: Do not enter the **erase /all nvram:** command. Rather, enter the **erase nvram** command to erase configuration files or the **delete nvram: file** command to delete individual files.

- CSCsg54522

Symptoms: A Security Device Event Exchange (SDEE) subscription request that does not contain an action is interpreted as an individual request rather than a subscription request.

Conditions: This symptom is observed on a Cisco router that is configured with the Cisco IOS Intrusion Prevention System (IPS).

Workaround: Ensure that the “action=get” action is contained in the subscription GET request.

- CSCsg55508

Symptoms: When you connect a cordless analog phone to the VIC-4FXS/DID Analog Voice Interface Card that is installed in a Cisco 1718, the phone does not ring when the Cisco 1700 series receives a call for phone. However, when you pick up the phone to answer the call, the call is correctly connected and managed.

Conditions: This symptom is observed on a Cisco 1718 running that runs Cisco IOS Release 12.3(11)T10, Release, 12.4, or Release 12.4T. The symptom does not occur on a Cisco 1751 that functions in the same configuration.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected voice port. Doing so enables the voice port to function properly until the router is reloaded, after which the symptom may occur again.

- CSCsg56423

Symptoms: A router that is configured with IPsec session may crash because of a bus error.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(6)T or a later release when there are two different IPsec sessions to different peers that protect the same traffic. The symptom may be triggered by clearing crypto sessions.

Workaround: There is no workaround.

- CSCsg56996

Symptoms: An H.323 gateway crashes after a memory leak exhausts all available memory.

Conditions: This symptom is observed when the following sequence of events occurs in a Unified Mobile Agent call flow that uses the nailed connection mode:

1. A mobile agent first logs onto a PSTN phone via a CTI port on the CallManager. This call remains active for the entire period that the mobile agent is active.
2. A new call from a customer comes in from the PSTN via another gateway, and after a call treatment, is redirected to the mobile agent. During this time, the initial call of the mobile agent is on hold.
3. When the call from the customer is redirected to the mobile agent, the RTP stream is sent to the phone of the mobile agent, which is then answered (that is, the phone is no longer on hold).
4. When the call of the customer is terminated, the initial call of the mobile agent is placed on hold again.

This situation causes a memory leak.

Workaround: There is no workaround.

- CSCsg57051

Symptoms: A provider edge (PE) router may not obtain label bindings from its Label Switch Controller (LSC), and the Tag-Controlled ATM (TC-ATM) process may not run on the PE router, which can be observed in the output of the **show processes | inc TC-** command. In addition, the log shows entries that are consistent with the symptom:

```
%TCATM-3-NOTRUNNING: ATM-TAGCONTROL is not running
```

Conditions: This symptom is observed when the PE router has an LC-ATM session with an LSC.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove all LC-ATM interfaces from the configuration by entering the **no interface type number** global configuration command for each LC-ATM interface. Then, reconfigure the LC-ATM interfaces.

- CSCsg58832

Symptoms: Inconsistent lease times may occur on a router that functions as a DHCP relay agent. The lease expiration times may be reduced from the value that is specified by the server to as little as five minutes. After the new lease time has expired, the binding is then deleted.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T, that is configured as a DHCP relay agent, and that has the **ip dhcp smart-relay** command enabled.

Workaround: Remove the **ip dhcp smart-relay** command from the configuration.

Alternate Workaround: Renew the IP address on the DHCP client.

- CSCsg65610

Symptoms: A Cisco 2611XM may reload when you enter the **show memory 0x6677ac48** command.

Conditions: This symptom is observed on a Cisco 2611XM that runs Cisco IOS Release 12.4 when the **service internal** command is enabled.

Workaround: There is no workaround.

Further Problem Description: The symptom does not occur on a Cisco 2651XM and Cisco 3825.

- CSCsg69124

Symptoms: A router crashes when the **write memory** and **secure boot-image** commands are executed simultaneously.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: There is no workaround.

Further Problem Description: Note that the commands must be entered simultaneously for the symptom to occur. When the commands are entered one after the other (in any order), the symptom does not occur.

- CSCsg69205

Symptoms: On a Cisco PE router that has the **ip flow egress** command enabled on an interface that connects to a CE router, the traffic streams that are destined for the CE router may not be captured.

Conditions: This symptom is observed when the MPLS interface is a multilink interface.

Workaround: Enter the **mpls netflow egress** command on the interface that connects the PE router to the CE router to enable the traffic streams to be captured by NetFlow. Once the traffic streams are being captured you can remove this command.

- CSCsg70932

Symptoms: A Cisco 7200 series that is configured for QoS may crash when traffic is sent.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or NPE-G2 and that has a Port Adapter Jacket Card in which a 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) is installed that has an interface with a service policy.

Workaround: There is no workaround.

- CSCsg75132

Symptoms: When the standby PRE comes up, the following error message is generated on the console of the active PRE:

```
REDUNDANCY-3-IPC: cannot open standby port session in use
```

Conditions: This symptom is observed on a Cisco 10000 series that has dual PRE engines that function in ISSU, RPR+, or SSO mode. The symptom may also occur on other platforms that support Enhanced High System Availability (EHSA) such as the Cisco 7304 and Cisco AS5850.

Workaround: There is no workaround.

Further Problem Description: The error message indicates that some of the Entity MIB information such as standby PRE version, standby flash information, and standby EEPROM data has failed to synchronize to the active PRE.

- CSCsg76519

Symptoms: An RSP may crash when you enter the **clear counters** command.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 when you enter the **clear counters** command after the termination of voice calls that were made with PA-VXC-2TE1 port adapters.

Workaround: There is no workaround.

- CSCsg76715

Symptoms: A device crashes when you delete an ACE that was inserted in the middle of the ACL rather than added at the end of the list.

Conditions: This symptom is observed when all of the following conditions are present:

- The inserted ACE has a destination prefix length of 0, that is, is has an “any” statement instead of a destination address.
- The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an “any” statement), and the inserted ACE has a lower sequence number than this other ACE.
- The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

Workaround: First, delete the inserted ACE. Then, delete the other ACE with the same SRC prefix length and an destination prefix length that is greater than 0.

Alternate Workaround: Delete the complete ACL.

- CSCsg78414

Symptoms: A sweep ping with a size of 4571 bytes may fail.

Conditions: This symptom is observed on a Cisco 7500 series when an ATM-IMA interface is configured with an MTU size of 7000 bytes.

Workaround: There is no workaround.

- CSCsg81585

Symptoms: After you stop sending stress traffic, an egress interface of an NM-4A/S stops sending all packets, that is, the output becomes stuck.

Conditions: This symptom is observed on a Cisco router when the following conditions are present:

- MLP is configured.
- There is an asynchronous physical layer on the serial interfaces.
- A dialer session is established by the stress traffic.

Workaround: Enter the **no ip route-cache** command on the egress interface of the NM-4A/S. Note that doing so may increase the CPU usage.

- CSCsg83834

Symptoms: A router may crash and generate an “%ALIGN-1-FATAL: Illegal access to a low address” error message.

Conditions: This symptom is observed on a Cisco router that is configured for IPv6, IPsec, and multicast.

Workaround: There is no workaround.

Further Problem Description: The fix for caveat CSCsg83834 also fixes caveat CSCsg94837. For more information about caveat CSCsg94837, see <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg94837>.

- CSCsg84909

Symptoms: When you enter the **format filesystem:** command or **delete URL /recursive** command, the image is deleted even though it is secured.

Conditions: This symptom is observed on a Cisco router that has an ATA file system.

Workaround: There is no workaround.

- CSCsg94951

Symptoms: When a router boots, a traceback is generated on the console.

Conditions: This symptom is observed on a Cisco 2600XM series, Cisco 2691, Cisco 3640, Cisco 3660, Cisco 3700 series, and Cisco 3800 series routers that run Cisco IOS interim Release 12.4(12.7) or a later release and in which an NM-2W, NM-1FE2W, NM-1FE1R2W, or NM-2FE2W network module is installed.

Note that the symptom may also occur on a Cisco 3660 router without the above-mentioned network modules because the on-board Fast Ethernet ports on the Cisco 3660 router share the same AMD chipset as the above-mentioned network modules.

Workaround: There is no workaround.

- CSCsg96462

Symptoms: A memory leak may occur in the SNASwitch process.

Conditions: This symptom is observed when the SNASwitch fails to free memory that is associated with maintaining the RTP history information when RTP pipes terminate under some conditions.

Workaround: There is no workaround.

Further Problem Description: The following messages may be generated when the processor memory has been exhausted:

```
%SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x6016CEA0, alignment
0
```

```
Pool: Processor Free: 1628716 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
-Process= "SNA Switch", ipl= 0, pid= 64
```

To check if memory is leaking, enter the following commands (note the exact upper/lower cases that are used):

```
show snasw rtp
show memory summary | i GraphIt | Bytes
```

The first command displays all the RTP pipes. The second command displays a summary of all the memory with a “GraphIt” identifier. There should be approximately two blocks with the “GraphIt Client” identifier for each non-RSETUP RTP pipe.

If there are significantly more than two “GraphIt Client” blocks per RTP pipe, the SNASwitch is leaking memory.

- CSCsg99155

Symptoms: When you configure an extended access control list (ACL) with the maximum sequence number and check the configuration with the **show access-list** command, the output does not show the maximum sequence number but a number that has one digit less than the configured maximum sequence number.

Conditions: This symptom is observed on a Cisco 7500 series that has an RSP. However, the symptom is platform-independent.

Workaround: There is no workaround.

- CSCsh05979

Symptoms: A VIP may reset because of a bus error when you remove a service policy from an ATM subinterface.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(20) but may also affect Release 12.4 and Release 12.4.T. The symptom appears to be platform-independent.

Workaround: There is no workaround.

- CSCsh11482

Symptoms: After you have reloaded the router or entered the **clear bgp ipv6 uni *** command, an incorrect link-local address of a next hop may be advertised for prefixes that are learned from the leader of update groups of the BGP Dynamic Update Peer-Groups feature.

Conditions: This symptom is observed on a Cisco platform that functions as a route-server and that has the same output policy for some eBGP peers.

Workaround: Use different output policies for all eBGP peers.

- CSCsh17884

Symptoms: A Cisco VoIP gateway with a T1 E&M trunk that is controlled by MGCP may reset because of a Restart in Progress (RSIP) situation or an out-of-service (OOS) state of the trunk.

Conditions: This symptom is observed on a Cisco VoIP gateway that interworks with a Cisco CallManager and uses MGCP E&M CAS trunks when a failure occurs for an outgoing call on the E&M trunk that generates a “wink down” event before an internal timer declares the wink timing invalid.

When you enable the **debug vpm signal** command, you can find the “wink down” event by searching in the output for “em_wink_timeout2”. Proper caution must be taken when enabling any debugs on a Cisco gateway. For example, at least you must disable console logging to minimize any performance impact.

Workaround: To prevent the symptom from occurring, enter the **timing wink-duration** voice-port (sub)command to change the timing of the “wink down” event. By default, this command is set to 200 msec, which means that the gateway expects the wink duration to be 200 msec and accepts any duration that is from 140 msec to 290 msec after the “wink up” event. By changing this value to, for example, 240 msec, the accepted duration becomes 180 msec to 330 msec. Basically, you want to match the wink timing characteristics of the switch equipment that is connected to the voice port.

When the symptom has occurred, enter the **shutdown** command followed a few seconds later by the **no shutdown** command on the affected voice port to enable the voice port to recover. Note that doing so causes all active calls on this voice port to be dropped.

When a single trunk is in the OOS state, entering the **no mgcp** command followed a few seconds later by the **mgcp** command may cause all trunks on the T1 link to enter the OOS state. Therefore, this command should not be used unless you use it after you have shut down and brought up the affected voice port.

- CSCsh20092

Symptoms: The value that is defined in the **config-register value** command may unexpectedly change on the standby eRSC.

Conditions: This symptom is observed on a Cisco AS5850 when you boot the eRSCs in RPR+ mode.

Workaround: There is no workaround.

- CSCsh20336

Symptoms: A spoke may be unable to connect or reconnect to a hub because there may not be a crypto socket.

Conditions: This symptom is observed in a DMVPN Hub-to-Spoke environment.

Workaround: Remove the static NHRP entry from the tunnel interface that connects the spoke to the hub, and reapply the static NHRP entry.

- CSCsh20354

Symptom 1: A third-party vendor VPN client may not be able to establish a VPN tunnel to a Cisco router. When you enable the **debug crypto isakmp** command on the Cisco router, the output shows the following:

```
ISAKMP:(0:4:HW:2):No IP address pool defined for ISAKMP!
ISAKMP:(0:4:HW:2):deleting SA reason "Fail to allocate ip address" state (R)
CONF_ADDR      (peer x.x.x.x)
```

Symptom 2: Although a third-party vendor VPN client can establish a VPN tunnel to a Cisco router, the client receives only an IP address but no DNS configuration, split-tunnel information, or other data during the mode configuration phase. In this situation, the debug output does not show any errors.

Conditions: Both of these symptoms are observed only when a third-party vendor VPN client connects to a Cisco router that functions as a VPN server.

Workaround: There are no workarounds.

- CSCsh21681

Symptoms: Immediately after you have configured a PRI group on a voice port adapter, the following error messages may be generated:

```
%VIP-3-BADMALUCMD
%Insufficient resources to create pri-group - it has been removed
```

Conditions: This symptom is observed on a Cisco 7500 series and is specific to the PA-VXC-2TE1+ and PA-VXB-2TE1+ port adapters. The symptom does not occur on the PA-MC-xT1, PA-MC-xE1, PA-MC-8TE1, and PA-MCX-8TE1+ port adapters.

Workaround: There is no workaround.

- CSCsh22978

Symptoms: The primary RSP may crash when you perform a soft OIR on the standby RSP.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMLP and RPR+.

Workaround: There is no workaround.

- CSCsh23176

Symptoms: A router crashes when you unconfigure RIP.

Conditions: This symptom is observed on a Cisco router and is more likely to occur when there are many RIP routes configured.

Workaround: Remove all network statements that are defined under the **router rip** command, wait for all RIP routes to age-out, then remove the **router rip** command.

- CSCsh24379

Symptoms: Traffic does not flow because of an incorrect VC, and an error message and traceback similar to the following may be generated:

```
%DMA-3-NO_VC: slot5: VIP2 R5K, Packet from FastEthernet0/0 to Serial1/1/0 has bad VC
8273, expected VC 133 adj VC 8273
%VIP-3-ERROR: slot5: VIP2 R5K,
-Traceback=
```

Conditions: This symptom is observed on a Cisco 7500 series that is configured for dFLioFR.

Workaround: There is no workaround.

- CSCsh33057

Symptoms: SPEs may hang after voice calls have been processed. When you enter the **clear spe** command for the affected SPEs, the platform may reload unexpectedly.

Conditions: These symptoms are observed on a Cisco AS5400 and Cisco AS5850.

Workaround: There is no workaround to prevent the SPEs from hanging. When the SPEs hang, reload the platform to recover the SPEs.

- CSCsh33429

Symptoms: A VIP crashes when you configure dFLioFR or dFLioATM.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 and that integrates the fix for caveat CSCsf25712. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf25712>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround.

- CSCsh42859

Symptoms: All interfaces may be lost on a Cisco 7500 series.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for SSO when you first remove any VIP via an OIR and then an SSO switchover occurs.

Workaround: There is no workaround.

- CSCsh58082

Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>.

- CSCsh71247

Symptoms: Cisco Express Forwarding (CEF) may not function correctly over PPP sessions, and the output of **show adjacency** command shows information similar to the following:

Protocol Interface Address IP Virtual-Access3 point2point(8) (incomplete)

Conditions: This symptom is observed on a Cisco router when PPP is used on a full virtual-access interface or multilink bundle.

Workaround: Disable CEF.

- CSCuk61396

Symptoms: WCCP service redirection may not work. In particular, packets that are rejected by a third-party vendor appliance device and are returned to the router for normal forwarding may be discarded.

Conditions: This symptom is observed on a Cisco router when NAT or Cisco IOS Firewall features are enabled on the same interfaces that have WCCP enabled.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsg39837

Symptoms: HTTP errors occur while accessing a Win2003 Web Server.

Conditions: This symptom has been observed with a Cisco IOS Voice gateway running Cisco IOS Release 12.4(6)T accessing a Win2003 HTTP web server under heavy load. Cisco IOS Voice has the **ip http client connection persistent** command disabled.

Workaround: There are two possible workarounds:

1. Switch to a Win2000 HTTP web server.
2. On a Win2003 server, set “TcpTimedWaitDelay” to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

- CSCsg61687

Symptoms: A router that has the **ip rcmd rsh-enable** command enabled may allow untrusted hosts to access the remote shell protocol (rsh) port.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(10.8)T3 but may also affect Release 12.4.

Workaround: Configure an access control list (ACL) to block rsh port 514 or disable rsh on the router. Note that as a result of this change, rsh and rcp connections from “nonprivileged” TCP ports will fail.

Wide-Area Networking

- CSCek59078

Symptoms: An L2TPv3 session is established when voluntary tunneling is configured and both peers have corresponding configurations. However, after you configure a pseudowire on a virtual PPP interface on one of the peers, the session on this peer is up but the line protocol is down, an a “virtual-PPP1 is up, line protocol is down” error message is generated.

Conditions: This symptom is observed when the virtual PPP interface is first deleted via the **no interface virtual-ppp number** command and then reconfigured via the **interface virtual-ppp number** command before you configure a pseudowire on the virtual PPP interface.

Workaround: Before you configure a pseudowire on the virtual PPP interface, ensure that the virtual PPP interface has never been unconfigured via the **no interface virtual-ppp number** configuration command.

- CSCek60025

Symptoms: A ping may be dropped in a PPP callback scenario.

Conditions: This symptom is observed on a Cisco router when Multilink PPP (MLP) and the **dialer load-threshold** command are enabled.

Workaround: There is no workaround.

- CSCek62099

Symptoms: When Multilink PPP (MLP) is enabled for a PPP over Ethernet (PPPoE) session, outbound packets are incorrectly sent without PPPoE headers. This situation causes packets to be dropped.

Conditions: This symptom is observed in Cisco IOS Release 12.4 on all software-forwarding routers and affects only packets that are not multilink-encapsulated (when the bundle has only a single link).

Workaround: Enter the **ppp multilink fragment delay** interface configuration command to force multilink headers to be applied to all outbound packets.

Alternate Workaround: Disable MLP.

- CSCsb24255

Symptoms: A router may generate the following error message and a MALLOC failure may occur:

```
flex_dsprm_voice_connect: voice tdm connect failed
```

Conditions: This symptom is observed on a Cisco router that processes a large number of calls with a short call duration via an E1 PRI.

Workaround: There is no workaround.

- CSCse38823

Symptoms: A multihop router may not establish a session that is initiated by a LAC, and a Call-Disconnect-Notify (CDN) message may be sent for one of the following reasons:

```
L2TP: disconnect (AAA) IETF: 15/service-unavailable Ascend: 67/VPDN Softshut/Session Limit
```

```
L2TP: disconnect (L2X) IETF: 9/nas-error Ascend: 62/VPDN No Resources
```

Conditions: This symptom is observed when the LAC is either a multihop LAC or a simple LAC that accepts dial-in calls, when the LAC has multiple destination LNSs configured in a VPDN group, and when the LNSs have a per VPDN-group session limit configured in the VPDN groups that accept the sessions from the LAC.

Workaround: Configure a minimal L2TP tunnel timeout value (5 seconds) in the VPDN group on the affected LAC by entering the **l2tp tunnel busy timeout 5** command.

First Alternate Workaround: Do not configure load-balancing.

Second Alternate Workaround: Create some loopback interfaces on the LNSs for different VPDN groups that the LAC can use, that is, configure different VPDN groups on the LAC that use distinct loopback addresses on the LNSs. When you do so and when a LAC receives a “busy” CDN message from an LNS, the LAC places only the particular address for the corresponding VPDN group on the LNS on the busy list without preventing VPDN groups of other LNSs to accept new sessions.

- CSCse66625

Symptoms: A router does not accept the **pppoe max-sessions number** command on a subinterface.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB but is not release-specific.

Workaround: First configure the **pppoe max-sessions** *number* command on a BBA group, then attach this BBA group to the subinterface.

- CSCsf30493

Symptoms: When a T.37 onramp call is made, the following error message may be generated:

```
%CSM-3-NO_VDEV: No modems associated
```

Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS interim Release 12.4(10.7). The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCsg34400

Symptoms: A Cisco router that functions as a LAC may crash.

Conditions: This symptom is observed when a PPPoE session is cleared by the client.

Workaround: There is no workaround.

- CSCsg38412

Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg40885

Symptoms: A router crashes during an online insertion and removal (OIR) of a multilink interface.

Conditions: This symptom is observed on a Cisco 7200 series that is configured for MLP and PPP.

Workaround: Shut down the multilink interface before you perform an OIR.

- CSCsg50202

Symptoms: When a BRI interface flaps rapidly, ISDN Layer 1 detects a link down state, but Layer 2 and Layer 3 may remain in the active state during the transition. This situation may cause the BRI interface to become stuck, and subsequent incoming and outgoing calls to be rejected.

Conditions: This symptom is observed when a cable is pulled out and put back rapidly.

Workaround: Enter the **clear interface** command on the affected BRI interface.

Alternate Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected BRI interface.

- CSCsg56148

Symptoms: Inbound GSM V.110 calls fail to train at a speed of 14400 bps.

Conditions: This symptom is observed on a Cisco AS5400 when the Bearer Capability (BC) does not match the Lower Layer Compatibility (LLC) in the ISDN setup message. The BC should take precedence over the LLC.

Workaround: If this an option, configure the ISDN switch to send the correct BC and LLC. If this is not an option, there is no workaround.

- CSCsg56725

Symptoms: When you enter the **terminate-from hostname** *host-name* command to terminate L2TP tunnels, some L2TP tunnels are terminated in the wrong VPDN group while other L2TP tunnels on the same host are terminated in the correct VPDN group.

Conditions: This symptom is observed on a Cisco 7206VXR router that has an NPE-G1 and that runs Cisco IOS Release 12.2SB and occurs only during the first two or three minutes after the router has booted. After that period, the symptom no longer occurs. Note that the symptom is both platform- and release-independent.

Workaround: To prevent the symptom from occurring, enter the **no aaa accounting system guarantee-first** command on the router before you reload the router. Doing so enables the tunnels to be terminated in the correct VPDN groups.

After the symptom has occurred, clear each of the affected tunnels by entering the **clear vpdn tunnel id** *local-id* command. Then, after the tunnels have been re-established, you should be able to terminate them in the correct VPDN groups.