Caveats for Cisco IOS Release 12.2

September 24, 2008

Cisco IOS Release 12.2(46a)

OL-3513-16 Rev. G0

This document lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.2, up to and including Cisco IOS Release 12.2(46a). 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 893.

Contents

- How to Use This Document, page 4
- If You Need More Information, page 5
- Resolved Caveats—Cisco IOS Release 12.2(46a), page 5
- Open Caveats—Cisco IOS Release 12.2(46), page 7
- Resolved Caveats—Cisco IOS Release 12.2(46), page 9
- Resolved Caveats—Cisco IOS Release 12.2(40a), page 13
- Resolved Caveats—Cisco IOS Release 12.2(40), page 19
- Resolved Caveats—Cisco IOS Release 12.2(37), page 21
- Resolved Caveats—Cisco IOS Release 12.2(34a), page 24
- Resolved Caveats—Cisco IOS Release 12.2(34), page 25
- Resolved Caveats—Cisco IOS Release 12.2(32), page 26
- Resolved Caveats—Cisco IOS Release 12.2(31), page 29

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

© 2001–2008 Cisco Systems, Inc. All rights reserved.

- Resolved Caveats—Cisco IOS Release 12.2(29b), page 32
- Resolved Caveats—Cisco IOS Release 12.2(29a), page 39
- Resolved Caveats—Cisco IOS Release 12.2(29), page 41
- Resolved Caveats—Cisco IOS Release 12.2(28d), page 47
- Resolved Caveats—Cisco IOS Release 12.2(28c), page 52
- Resolved Caveats—Cisco IOS Release 12.2(28b), page 52
- Resolved Caveats—Cisco IOS Release 12.2(28a), page 53
- Resolved Caveats—Cisco IOS Release 12.2(28), page 54
- Resolved Caveats—Cisco IOS Release 12.2(27c), page 61
- Resolved Caveats—Cisco IOS Release 12.2(27b), page 68
- Resolved Caveats—Cisco IOS Release 12.2(27a), page 69
- Resolved Caveats—Cisco IOS Release 12.2(27), page 71
- Resolved Caveats—Cisco IOS Release 12.2(26c), page 81
- Resolved Caveats—Cisco IOS Release 12.2(26b), page 88
- Resolved Caveats—Cisco IOS Release 12.2(26a), page 89
- Resolved Caveats—Cisco IOS Release 12.2(26), page 93
- Resolved Caveats—Cisco IOS Release 12.2(24b), page 102
- Resolved Caveats—Cisco IOS Release 12.2(24a), page 105
- Resolved Caveats—Cisco IOS Release 12.2(24), page 106
- Resolved Caveats—Cisco IOS Release 12.2(23f), page 117
- Resolved Caveats—Cisco IOS Release 12.2(23e), page 118
- Resolved Caveats—Cisco IOS Release 12.2(23d), page 121
- Resolved Caveats—Cisco IOS Release 12.2(23c), page 123
- Resolved Caveats—Cisco IOS Release 12.2(23a), page 123
- Resolved Caveats—Cisco IOS Release 12.2(23), page 128
- Resolved Caveats—Cisco IOS Release 12.2(21b), page 141
- Resolved Caveats—Cisco IOS Release 12.2(21a), page 145
- Resolved Caveats—Cisco IOS Release 12.2(21), page 147
- Resolved Caveats—Cisco IOS Release 12.2(19c), page 161
- Resolved Caveats—Cisco IOS Release 12.2(19b), page 163
- Resolved Caveats—Cisco IOS Release 12.2(19a), page 167
- Resolved Caveats—Cisco IOS Release 12.2(19), page 168
- Resolved Caveats—Cisco IOS Release 12.2(17f), page 192
- Resolved Caveats—Cisco IOS Release 12.2(17e), page 192
- Resolved Caveats—Cisco IOS Release 12.2(17d), page 196
- Resolved Caveats—Cisco IOS Release 12.2(17b), page 200
- Resolved Caveats—Cisco IOS Release 12.2(17a), page 200
- Resolved Caveats—Cisco IOS Release 12.2(17), page 202

- Resolved Caveats—Cisco IOS Release 12.2(16f), page 232
- Resolved Caveats—Cisco IOS Release 12.2(16c), page 236
- Resolved Caveats—Cisco IOS Release 12.2(16b), page 237
- Resolved Caveats—Cisco IOS Release 12.2(16a), page 239
- Resolved Caveats—Cisco IOS Release 12.2(16), page 244
- Resolved Caveats—Cisco IOS Release 12.2(13e), page 293
- Resolved Caveats—Cisco IOS Release 12.2(13c), page 297
- Resolved Caveats—Cisco IOS Release 12.2(13b), page 300
- Resolved Caveats—Cisco IOS Release 12.2(13a), page 302
- Resolved Caveats—Cisco IOS Release 12.2(13), page 306
- Resolved Caveats—Cisco IOS Release 12.2(12m), page 355
- Resolved Caveats—Cisco IOS Release 12.2(12l), page 355
- Resolved Caveats—Cisco IOS Release 12.2(12k), page 359
- Resolved Caveats—Cisco IOS Release 12.2(12j), page 360
- Resolved Caveats—Cisco IOS Release 12.2(12i), page 362
- Resolved Caveats—Cisco IOS Release 12.2(12h), page 364
- Resolved Caveats—Cisco IOS Release 12.2(12g), page 369
- Resolved Caveats—Cisco IOS Release 12.2(12f), page 370
- Resolved Caveats—Cisco IOS Release 12.2(12e), page 370
- Resolved Caveats—Cisco IOS Release 12.2(12c), page 371
- Resolved Caveats—Cisco IOS Release 12.2(12b), page 372
- Resolved Caveats—Cisco IOS Release 12.2(12a), page 379
- Resolved Caveats—Cisco IOS Release 12.2(12), page 381
- Resolved Caveats—Cisco IOS Release 12.2(10g), page 445
- Resolved Caveats—Cisco IOS Release 12.2(10d), page 450
- Resolved Caveats—Cisco IOS Release 12.2(10b), page 454
- Resolved Caveats—Cisco IOS Release 12.2(10a), page 456
- Resolved Caveats—Cisco IOS Release 12.2(10), page 458
- Resolved Caveats—Cisco IOS Release 12.2(7g), page 535
- Resolved Caveats—Cisco IOS Release 12.2(7e), page 535
- Resolved Caveats—Cisco IOS Release 12.2(7c), page 536
- Resolved Caveats—Cisco IOS Release 12.2(7b), page 538
- Resolved Caveats—Cisco IOS Release 12.2(7a), page 541
- Resolved Caveats—Cisco IOS Release 12.2(7), page 541
- Resolved Caveats—Cisco IOS Release 12.2(6j), page 592
- Resolved Caveats—Cisco IOS Release 12.2(6i), page 593
- Resolved Caveats—Cisco IOS Release 12.2(6h), page 594
- Resolved Caveats—Cisco IOS Release 12.2(6g), page 595

- Resolved Caveats—Cisco IOS Release 12.2(6f), page 597
- Resolved Caveats—Cisco IOS Release 12.2(6e), page 598
- Resolved Caveats—Cisco IOS Release 12.2(6d), page 599
- Resolved Caveats—Cisco IOS Release 12.2(6c)M1, page 601
- Resolved Caveats—Cisco IOS Release 12.2(6c), page 601
- Resolved Caveats—Cisco IOS Release 12.2(6b), page 602
- Resolved Caveats—Cisco IOS Release 12.2(6a), page 604
- Resolved Caveats—Cisco IOS Release 12.2(6), page 605
- Resolved Caveats—Cisco IOS Release 12.2(5d), page 645
- Resolved Caveats—Cisco IOS Release 12.2(5c), page 645
- Resolved Caveats—Cisco IOS Release 12.2(5a), page 645
- Resolved Caveats—Cisco IOS Release 12.2(5), page 646
- Resolved Caveats—Cisco IOS Release 12.2(3g), page 681
- Resolved Caveats—Cisco IOS Release 12.2(3d), page 681
- Resolved Caveats—Cisco IOS Release 12.2(3b), page 681
- Resolved Caveats—Cisco IOS Release 12.2(3a), page 682
- Resolved Caveats—Cisco IOS Release 12.2(3), page 683
- Resolved Caveats—Cisco IOS Release 12.2(2), page 853
- Resolved Caveats—Cisco IOS Release 12.2(1)M0, page 853
- Resolved Caveats—Cisco IOS Release 12.2(1d), page 853
- Resolved Caveats—Cisco IOS Release 12.2(1c), page 854
- Resolved Caveats—Cisco IOS Release 12.2(1b), page 854
- Resolved Caveats—Cisco IOS Release 12.2(1a), page 856
- Resolved Caveats—Cisco IOS Release 12.2(1), page 860
- Obtaining Documentation and Submitting a Service Request, page 893

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, AppleTalk caveats are listed separately from, and before, IP caveats. The caveats are also sorted alphanumerically by caveat number.

If You Need More Information

Cisco IOS software documentation can be found on the web through Cisco.com. For information on Cisco.com, see the "Obtaining Documentation and Submitting a Service Request" section on page 893.

For more information on caveats and features in Cisco IOS Release 12.2, refer to the following sources:

- Dictionary of Internetworking Terms and Acronyms—The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this caveats document.
- Bug Toolkit—If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
- Release Notes for Cisco IOS Release 12.2—These release notes describe new features and significant software components for Cisco IOS software Release 12.2.
- Deferral Advisories and Software Advisories for Cisco IOS Software—*Deferral Advisories and Software Advisories for Cisco IOS Software* provides information about caveats that are related to deferred software images for Cisco IOS releases. If you have an account on Cisco.com, you can access *Deferral Advisories and Software Advisories for Cisco IOS Software* at http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml.
- What's New for IOS—*What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml.
- Cisco IOS Software Roadmap—The *Cisco IOS Software Roadmap* illustrates the relationship of the various Cisco IOS releases. If you have an account on Cisco.com, you can access the *Cisco IOS Software Roadmap* at http://www.cisco.com/warp/customer/620/roadmap_b.shtml.

The most recent release notes when this caveats document was published were Release Notes for Cisco IOS Release 12.2, for Cisco IOS Release 12.2(46) on April 27, 2007.

Resolved Caveats—Cisco IOS Release 12.2(46a)

Cisco IOS Release 12.2(46a) is a rebuild release for Cisco IOS Release 12.2(46). The caveats in this section are resolved in Cisco IOS Release 12.2(46a) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- 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

- 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

- CSCsi74508

  Symptoms: A Cisco IOS device may produce the following error when reading or writing the configuration:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: write of 11 bytes to 10 bytes
  ```

  Conditions: This symptom has been observed when reading or writing the configuration.

  Workaround: There is no workaround.

- CSCsi78162

  Symptoms: A router that has the SNASwitch feature enabled may generate several of the following messages along with tracebacks:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy of xx bytes should be xx bytes
  ```

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCsh87705. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh87705. 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.

  Further Problem Description: The messages do not affect the normal operation of the router in any way. The SNASwitch continues to function normally.

- CSCsj16292

  Symptoms: Following an upgrade to Cisco IOS Release 12.2(18)SXF9, the following message may be displayed:

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

  Conditions: This message may appear as a result of SNMP polling of PAgP variables, but does not appear to be service impacting.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCeh48684

  Symptoms: Identification field is always 0 in the tacacs+ packet with SYN flag. The TACACS packet goes from a Catalyst 6509 through an FW to the AAA server. The FW construes this as a Fragment Overlap Attack and drops additional new connections.

  Conditions: This symptom has been observed on a Catalyst 6509 connecting through an FW to an AAA server.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(46)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(46). All the caveats listed in this section are open in Cisco IOS Release 12.2(46). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCse80032

  Symptoms: An SNMP Manager that uses SNMPv3 may not resynchronize the timer for the SNMP engine after the router has been reloaded.

  Conditions: This symptom is observed on Cisco Catalyst 6000 series switch and Cisco 7600 series router that have been reloaded and occurs because a parameter is incorrectly set in the REPORT message, causing a mediation device to register an SNMP timeout instead of a reload.

  Workaround: You may be able to restart the SNMP Manager to force the timer for the SNMP engine to resynchronize. Note, however, that doing so causes a 100-percent outage for all wiretaps that are served by the SNMP Manager. If you cannot restart the SNMP Manager, there is no workaround.

IP Routing Protocols

- CSCsg51897

  Symptoms: Rate limiting feature with MQC does not work on a multilink interface on an RSP router that is configured with MDS with the policy applied as an output policy. Because of this, traffic is not rate limited, and all traffic passes through.

  Conditions: This symptom is observed on an RSP router that is running Cisco IOS Interim Release 12.4(11.6a).

  Workaround: There is no workaround.

Miscellaneous

- CSCea53765

  Symptoms: Adding a /31 netmask route on a Cisco router may not overwrite an existing /32 CEF entry.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1(13)E4, Release 12.2 other 12.1 E releases, or Release 12.3.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables prefixes that are derived from adjacencies in the FIB to be periodically validated against covering prefixes that originate from the RIB. Validation ensures that an adjacency prefix is only active when it points out of the same interface as a covering attached prefix. To enable this validation, enter the **ip cef table adjacency-prefix validate** global configuration command.

  Note that because validation is periodic, there could be a time lag between RIB changes and subsequent validation or withdrawal of covered adjacencies in the FIB.

- CSCin86002

  Symptoms: The bandwidth of an IMA group interface may be less than the combined bandwidth of its active member links that are up and operational.

  Conditions: This symptom is observed on an IMA group interface of a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter that is installed in a Cisco 7xxx platform when the IMA group interface has more than one member link. The symptom occurs when you enter the shutdown

interface configuration command quickly followed by the no shutdown interface configuration command on a member link (that is, the command sequence takes less than two seconds). When the member link comes up, the bandwidth of the IMA group interface is not increased.

Workaround: There is no workaround.

- CSCsh61946

  Symptoms: After an SSO switchover has occurred, the second of two 6000 W DC power supplies in the chassis is shut down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 router when both power supplies are powered on before the SSO switchover occurs.

  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.

- CSCsi51581

  Symptoms: A VIP4-80 that is running Cisco IOS Release 12.2(40) crashes due to a software bus error.

  Conditions: This symptom is observed when a VIP4-80 crashes while all interfaces are coming up.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(46)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(46). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(46). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCeg62070

  Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

  Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

  Workaround: Disable HTTP server using the **no ip http server** command.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

IP Routing Protocols

- CSCsi23231

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 (registered customers only) for non-12.2 mainline releases and CSCsi23231 (registered customers only) for 12.2 mainline releases.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCeb21064

  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

- CSCin83971

  Symptoms: Voice calls with ground-start signaling fail at the terminating gateway (TGW) with confirmed errors at the originating side.

  Conditions: This symptom is observed when the dial peers are matched, when VTSP initiates dialing the remote destination, when the DSP fails to wait for the offhook signal transition from the remote endpoint, and when the DSPRM closes the DSP voice channel.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected voice port on the TGW. Note that the symptom does not occur with loop-start signaling.

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

  Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsb40304

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- 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

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml.

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the Cisco IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

Resolved Caveats—Cisco IOS Release 12.2(40a)

Cisco IOS Release 12.2(40a) is a rebuild release for Cisco IOS Release 12.2(40). The caveats in this section are resolved in Cisco IOS Release 12.2(40a) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCeg62070

  Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

Workaround: Disable HTTP server using the **no ip http server** command.

- CSCse04560

Symptoms: A tftp client trying to transfer a file from a Cisco IOS device configured as a tftp server and which is denied by an ACL receives a different result depending if the file is being offered for download or not. This may allow a third party to enumerate which files are available for download.

Conditions: The **tftp-server** command is configured on the device and an ACL restricting access to the file in question has been applied as in this example:

```
tftp-server flash:filename1 access-list-number
access-list access-list- number
   permit 192.168.1.0 0.0.0.255
access-list access-list- number
   deny any
```

Workaround: The following workarounds can be applied:

1. Interface ACL Configure and attach an access list to every router interface active and configured for IP packet processing. Example:

```
access-list access-list- number
   remark --- the following hosts and networks area ALLOWED for TFTP access
access-list access-list- number
   permit udp host source_1
   host interface_address_1
   eq 69
access-list access-list- number
   permit udp host source_2
   host interface_address_2
   eq 69
access-list access-list- number
   permit udp source source- wildcard
   host interface_address_1
   eq 69
access-list access-list- number
   permit udp source source- wildcard
   host interface_address_2
   eq 69
access-list access-list- number
   remark --- everyone else is DENIED for TFTP access
access-list access-list- number
   deny udp any host interface_address_1
   eq 69
access-list access-list- number
   deny udp any host interface_address_2
   eq 69
access-list access-list- number
   remark --- any other traffic to/through the router is allowed
access-list access-list- number
   permit ip any any
   interface Ethernet0/0
   ip access-group access-list- number in
```

Once the tftp server in Cisco IOS is enabled and listening by default on all interfaces enabled for IP processing, the access list would need to deny traffic to each and every IP address assigned to any active router interface.

2. Control Plane Policing Configure and apply a CoPP policy. For example:

```
access-list access-list- number
```

```
   remark --- Do not police TFTP traffic from trusted hosts and networks
access-list access-list- number
   deny udp host source_1 any eq 69
access-list access-list- number
   deny udp source source- wildcard any eq 69
access-list access-list- number
   remark --- Police TFTP traffic from untrusted hosts and networks
access-list access-list- number
   permit udp any any eq 69
access-list access-list- number
   remark --- Do not police any other traffic going to the router
access-list access-list- number
   deny ip any any
class-map match-all tftp- class
   match access-group access-list- number
policy-map control-plane- policy
   ! Drop all traffic that matches the class tftp- class
   class tftp- class
      drop
control-plane service-policy input control- plane- policy
```

Note: CoPP is only available on certain platforms and Cisco IOS releases. Additional information on the configuration and use of the CoPP feature can be found at the following URL: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

3. Infrastructure ACLs (iACL) Although often difficult to block traffic transitting your network, identifying traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network is possible. Infrastructure 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 iACLs: http://www.cisco.com/warp/public/707/iacl.html

4. Configuring Receive Access Lists (rACLs) For distributed platforms, rACLs may be an option starting in Cisco IOS Release 12.0(21)S2 for the Cisco 12000 series GSR and Cisco IOS Release 12.0 (24)S for the Cisco 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path 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 CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets: http://www.cisco.com/warp/public/707/racl.html

NOTE: The suggested workarounds are an "all or nothing" solution. While the tftp-server feature in Cisco IOS allows per-file ACLs to be attached to every file being offered for download, the suggested workarounds are global and will either prevent or allow access to all files being shared. It is recommended to apply the suggested workarounds in addition to the existing per-file ACLs, instead of replacing them.

- CSCsg70355

  Symptoms: Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

  Conditions: The Cisco IOS configuration command:

  clock summer-time *zone* **recurring**

uses United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March. It changes the end date from the last Sunday of October to the first Sunday of November.

Workaround: A workaround is possible by using the **clock summer- time** configuration command to manually configure the proper start date and end date for daylight savings time. After the summer-time period for calendar year 2006 is over, one can for example configure:

clock summer-time *PDT* **recurring** *2 Sun Mar 2:00 1 Sun Nov 2:00*

(This example is for the US/Pacific time zone.)

Not A Workaround: Using NTP is not a workaround to this problem. NTP does not carry any information about timezones or summertime.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

Miscellaneous

- CSCeb21064

  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

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsb40304

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- 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

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the Cisco IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

TCP/IP Host-Mode Services

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  - The router must have RCP enabled.
  - The packet must come from the source address of the designated system configured to send RCP packets to the router.
  - The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

Resolved Caveats—Cisco IOS Release 12.2(40)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(40). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(40). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCse85200

  Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

  Workaround: Disable on interfaces where CDP is not necessary.

Miscellaneous

- CSCsd80754

  Symptoms: The active router in an HSRP configuration may not respond to an ARP request for the virtual IP address. When the symptom occurs, both routers in the HSRP configuration have correct HSRP and ARP entries. Entering the **clear arp** command on the standby router in the HSRP configuration does not resolve the problem.

  Conditions: This symptom is observed when the same HSRP virtual IP address exists in different HSRP groups on different routers.

  Workaround: Enter the **no standby redirects** command to prevent the symptom from occurring.

- CSCse68138

  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

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCuk57037

  Symptoms: A router may crash when a serial interface of a neighboring router is brought up.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that is earlier than Release 12.4(8) and that is configured for IP Multicast when some interfaces on the router are configured for PIM. The symptom occurs when the serial interface that is brought up on the neighboring router is configured for PIM and the connecting interface on the Cisco router is not configured for PIM.

  Workaround: Depending on the desired operation for the link, either enable PIM at both ends or disable PIM at both ends.

Resolved Caveats—Cisco IOS Release 12.2(37)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(37). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(37). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCef68681

  Symptoms: A CBUS complex may occur, causing all VIPs to reload and to be reconfigured. In turn, this situation prevents the router from being accessible for 30 seconds.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when you change the MTU of an already existing interface or when you add a new interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg11566

  Symptoms: Intensive SNMP polling may cause the I/O memory of a router to be depleted.

  Conditions: This symptom is observed in rare situations.

  Workaround: Reduce the SNMP polling interval, frequency, or rate.

- CSCej57779

  Symptoms: A reload of a Cisco 7600 router, with a huge number (for example, 1000) of VRF configured with BGP/VPN learning redistributed routers, may cause some VRFs to not learn distributed routes from the peer.

  Conditions: This symptom has been observed in Cisco IOS Release 12.2SRA when a huge number of VRF are configured. This symptom is not applicable to Cisco IOS Release 12.4.

  Workaround: The symptom can be resolved on the per VRF basis by removing the VRF instance and the BGP/VPN configuration for this instance and then adding them back.

IP Routing Protocols

- CSCee36622

  Symptoms: ABRs may continue to generate summary LSA(s) for obsolete non-backbone intra-area route(s).

  Conditions: This symptom occurs under the following conditions:

  1. The ABR (call ABR X) has at least one non-backbone area (call area X) in common with one or more additional ABRs.
  2. The ABRs are generating summary LSAs, on behalf of the Area X's two or more intra-area routes, into the backbone area and other areas. The two intra-area routes must be advertised as stub links from two different routers; i.e., one from ABR X, and the other from another router belonging to Area X.
  3. The summary LSA IDs for the intra-area routes above, when ORed with the host bits of the corresponding masks, yield identical LSA IDs.

  For example, 10.10.10.128/25 and 10.10.10.0/24 yield identical

  LSA IDs when the network address is logically ORed with the

  host bits; i.e.,

  10.10.10.128 | 0.0.0.127 = 10.10.10.255

  10.10.10.0 | 0.0.0.255 = 10.10.10.255

  Workaround: Perform the **clear ip ospf proc** command on all ABRs containing the obsolete LSAs.

Miscellaneous

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCef50713

  Symptoms: Traffic may be duplicated when it passes through HSRP-enabled interfaces.

  Conditions: This symptom is observed on a Cisco 2600 series that is configured with a Fast Ethernet interface that contain an AM79c971 chip when the connected hub is a layer 2 device (not a switch).

  Workaround: Replace the hub with a switch or enter the **standby use-bia** command on the Fast Ethernet interface.

  Further Problem Description: When HSRP enters the standby state after the router has reloaded, the Fast Ethernet interface enters the non-promiscuous mode. When HSRP becomes active on the router, the Fast Ethernet interface enter the promiscuous mode but remains in this mode even when HSRP enters the standby state again.

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

- CSCin31767

  Symptoms: A Cisco router may reload when you enter the **show atm map** privileged EXEC command.

  Conditions: This symptom is observed on all Cisco routers after you have first deleted a subinterface on which a static map bundle was configured.

  Workaround: First remove the static map bundle; then, delete the subinterface.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

Workaround: There is no workaround.

- CSCsd43501

  Symptoms: Voice over Frame Relay (VOFR) Connection PLAR calls that are configured for FXS fail with tracebacks on a Cisco 7200 originating gateway.

  Conditions: This issue is seen when the Cisco 7200 gateway is configured with FXS loopstart or ground start signaling.

  Workaround: There is no workaround.

- CSCsd81861

  Symptoms: A router may unexpectedly reload due to a bus error after being reloaded or power cycled. The last console output in the crashinfo will be the **ima-group** *group number* command before the crash.

  Conditions: The router must have the **ip telnet source- interface** command or the **ip tftp source-interface** command configured to use an IMA sub-interface as the source. There also must be at least one ATM interface in the IMA group.

  Workaround: Remove the IMA interface from the **source interface** command in the configuration.

Resolved Caveats—Cisco IOS Release 12.2(34a)

Cisco IOS Release 12.2(34a) is a rebuild release for Cisco IOS Release 12.2(34). The caveats in this section are resolved in Cisco IOS Release 12.2(34a) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCse08786

  This DDTS documents changes in how IOS handles packets destined to the router or switch.

Resolved Caveats—Cisco IOS Release 12.2(34)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(34). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(34). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml.

Interfaces and Bridging

- CSCin51588

  Symptoms: When you reload the microcode onto an enhanced 8-port multichannel T1/E1 port adapter (PA-MC-8TE1+) while traffic is flowing through the port adapter, the following error message may appear:

```
%RSP-3-RESTART: interface Serial0/0/4:0, not transmitting
```

In most cases, the interfaces of the port adapter recover on their own. In very rare cases, the execution of a Cbus Complex occurs.

Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: If the interfaces of the port adapter do not recover on their own, execute a Cbus Complex.

- CSCsc61784

  Symptoms: The **show interface** *interface* **stats** command output incorrectly shows fastswitched packets as process switched packets.

  Conditions: This symptom is observed on a Cisco 7200 platform on T1/E1 interfaces only.

  Workaround: There is no workaround. Do not rely on the counters displayed by the **show interface** *interface* **stats** command output.

Miscellaneous

- CSCeg67788

  Symptoms: The 5-minute output rate in the output of the **show interfaces** command is incorrect for serial interfaces that are configured on a PA-MC-8TE1+ port adapter.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8TE1+ port adapter.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(32)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(32). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(32). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCea56560

  Symptoms: Configuring nonexisting NTP peers repeatedly over a period of time may cause a system reload.

  Conditions: This symptom may occur on any Cisco Catalyst Switch that is running Cisco IOS releases, but is not platform dependent.

  Workaround: Avoid adding/deleting nonexisting NTP peers in quick succession, for example using cut-and-paste.

Interfaces and Bridging

- CSCin67809

  Symptoms: CEF, dCEF, and fast-switching counters are not accurate on outbound serial E1 or T1 interfaces.

  Conditions: This symptom is observed on a Cisco 7200 series when CEF, dCEF, and fast-switching are enabled on a serial E1 or T1 interface.

  Workaround: There is no workaround.

Miscellaneous

- CSCee20451

  Symptoms: A VC may experience an output stuck condition.

  Conditions: This symptom occurs when using T1 ATM (the IMA function is not used) on a PA-A3-8T1IMA.

  Workaround: Perform the **clear interface** command.

- CSCeh78918

  Symptoms: When a line card has reloaded because you reloaded the router, the line card crashed, or you entered a command to reload the line card, the following message may appear on the console:

  ```
  %MDS-2-RP: MDFS is disabled on some line card(s). Use "show ip mds stats linecard" to
  view status and "clear ip mds linecard" to reset.
  ```

  This message may be generated because MDFS is erroneously disabled on the reloaded line card. Erroneous disabling of MDFS may unnecessarily extend network convergence time.

  Conditions: This symptom is observed on a distributed router or switch such as a Cisco Catalyst 6000 series, Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series. The symptom occurs when the router has the **ip multicast-routing distributed** command enabled for any VRF and when a line card is reloaded more than 50 seconds into the 60-second MDFS flow-control period.

  Workaround: The symptom corrects itself after 60 seconds. Alternatively, you can enter the **clear ip mds linecard** *slot number* command.

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb18502

  Symptoms: Data that is forwarded downstream from a SNASw router is intermittently corrupted. Sniffer traces that are captured upstream and downstream from the SNASw router show that the data that is sent from the host to the SNASw router is fine, but when the data leaves the SNASw router, there are some corrupted bytes at the end of the data stream.

Conditions: This symptom is observed on a SNASw router that is connected upstream to a mainframe host via Enterprise Extender.

Workaround: There is no workaround.

- CSCsb99091

  Symptoms: An SNA Switch (SNASw) router reloads in snaswitch code in case of memory shortage.

  Conditions: This symptom was observed with a router that is concentrating downstream physical units (DSPU) via DLSw/VLDC, and forwarding their traffic via HPR/LLC to the mainframes. There are about 300 to 400 physical units concentrated via the SNASw/DLUR. There are total of 16 routers in this system, with pairs of 8 routers backing up each other.

  Workaround: There is no workaround.

- CSCsc02139

  Symptoms: A router running SNA Switch (SNASw) may reload unexpectedly after logging the following messages:

  ```
  Sep 13 08:42:45.950 METDST: %SNASW-3-SM_LOG_5: PROBLEM - 287990 - Insufficient storage
  to activate LU6.2 session
  Sep 13 08:42:46.014 METDST: %SNASW-3-SS_LOG_16: PROBLEM - 287994 - CP capabilities
  exchange failed because of contention winner CP-CP session failure
  Sep 13 08:42:47.946 METDST: %SNASW-3-SS_LOG_16: PROBLEM - 288001 - CP capabilities
  exchange failed because of contention winner CP-CP session failure (Message suppressed
  16 times) Sep 13 08:42:47.946 METDST: %SNASW-3-SM_LOG_5: PROBLEM - 287991 -
  Insufficient storage to activate LU6.2 session (Message suppressed 109 times)

  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x61327E00
  ```

  Conditions: This symptom has been observed on a DLSw/SNASw concentration router which is providing connectivity for 300 to 400 physical units through DLSw.

  Workaround: There is no workaround.

- CSCsc25745

  Symptoms: In rare circumstances, an SNA Switch (SNASw) may get a “half session” towards the backup DLUS; issuing the **show snasw session local** command, and verifying the details that there is a CONWINNER, but no CONLOSER. On the mainframe side, the link appears to hang.

  This creates no problem in operation, except when issuing a **GiveBack** command or a **Takeover** command, in which case, the link towards the backup DLUS does not work.

  Conditions: This symptom has been observed on a Cisco 7200 router with an SNASw.

  Workaround: The situation can be cleared with a **snasw stop session** *pcid* using the PCID shown with the **show snasw session local** command.

Wide-Area Networking

- CSCsc08345

  Symptoms: A Cisco router may crash unexpectedly due to a bus error when it dereferences a pointer to freed memory in one of the error paths in TCP-to-PAD translation.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(31). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(31). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

IBM Connectivity

- CSCeh18295

  Symptoms: DLSw circuits do not connect.

  Conditions: This symptom is observed when DLSw Ethernet redundancy is configured via the **dlsw transparent switch-support** command.

  Workaround: Recycle DLSw on the master router.

  Further Problem Description: The output of the **show dlsw transparent cache** command shows the NEGATIVE state for the circuits on the master router although no actual circuits exist on either the master router or the slave router.

- CSCeh90809

  Symptoms: Removing BSTUN peer attribute causes a Cisco router to crash.

  Conditions: This symptom occurs when changing the **bstun protocol- group** *protocol name* global configuration command and subsequently changing the **bsc char-set** value (from ascii to ebcdic or vice versa) on the BTSUN encapsulated interface. The router will crash.

  Workaround: There is no workaround.

Miscellaneous

- CSCea84387

  Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive.

  Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions.

  Workaround: Allow only one user at a time to enter MQC commands.

- CSCeb47225

  Symptoms: If a key is configured on a tunnel interface, the inbound access-list on that interface is ignored.

  Conditions: This problem is seen with a configuration that is similar to the following:

```
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 100 in
 tunnel source FastEthernet0/0
```

```
 tunnel destination 172.16.1.1
 tunnel key 1
end
```

This problem does not occur if "tunnel key" is not configured.

Workaround: Remove the "tunnel key."

- CSCed83616

  Symptoms: A Cisco router may reload when you enter the **show standby** or **show standby brief** command.

  Conditions: This symptom is observed on a Cisco Multiprocessor WAN Application Module MWAM) when multiple HSRP groups are configured and unconfigured in a loop while traffic for the HSRP groups is being processed. The symptom may be platform-independent.

  However, a stress scenario in which many HSRP groups are configured and unconfigured while the **show standby** or **show standby brief** command is executed may be a rather uncommon scenario.

  Workaround: Do not to enter the **show standby** or **show standby brief** command while configuration changes are being made.

- CSCed90476

  Symptoms: Unable to configure framing CRC4 (Australian) on a Channelized E1.

  Conditions: This symptom is observed on a Cisco 10000 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCee41831

  Symptoms: A SegV exception may occur on a router when you enter the **write memory** or **copy running-config startup-config** command.

  Conditions: This symptom is observed on a Cisco 1700 series and Cisco 2600 series when you enter the **write memory** or **copy running-config startup-config** command and when the NVRAM is corrupted.

  Workaround: Erase the NVRAM and then enter the **write memory** or **copy running-config startup-config** command.

- CSCef08173

  Symptoms: VIP with PA-2FE may reload due to memory corruption caused by PA-2FE hardware.

  Conditions: This problem is triggered when VIP/PA is stressed, VIP is not able to serve memory read/write request from PA hardware, and there are PCI retry timeouts.

  Workaround: There is no workaround.

- CSCeg36362

  Symptoms: A Cisco 7200 series that is configured with an NPE-G1 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when the Cisco 7200 series is configured for Fast Switching.

  Workaround: There is no workaround.

- CSCeg86187

  Symptoms: The **ip mroute-cache distributed** interface configuration command is not retained after you reload a router.

  Conditions: This symptom is observed on a Cisco 7500 series.

Workaround: After the router has reloaded, reconfigure the **ip mroute-cache distributed** interface configuration command on each affected interface.

- CSCeh17756

  Symptoms: The PIM assert mechanism may not function properly, causing PE routers to remove VRF subinterfaces from output interface lists, and, in turn, causing multicast traffic to be dropped.

  Conditions: This symptom is observed when redundant PE routers and CE routers are located on one LAN segment and when the CE routers select different PE routers as their next hop.

  Workaround: Change the configuration in such a way that all CE routers on one LAN segment select the same PE router as their next hop.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCin55942

  Symptoms: When you enter the **channel-group** command, a router may crash.

  Conditions: This symptom is observed when you enter the **channel-group** command on native FE interfaces on a Cisco 3660 router or on NM-xFE interfaces on a Cisco 3600 series or Cisco 3700 series.

  The **channel-group** command should not be used on native FE ports or on NM-FE ports because it is not supported on these ports. The **channel-group** command is meant only for NM-1GE GE ports and switching FE ports.

  Workaround: There is no workaround. The fix for this DDTS ensure that the router does not crash. However, the EtherChannel is not supported on native FE ports and NM-xFE ports on a Cisco 3600 series and Cisco 3700 series.

- CSCin81933

  Symptoms: At a cold temperature, a Cisco 7200 series does not boot with a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter and generates a watchdog timeout error.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-300 or NPE-400 and an IMA port adapter.

  Workaround: There is no workaround.

- CSCin93609

  Symptoms: A Cisco 7200 series or Cisco 7500 series may crash when bridged PVCs are deleted and added to an IMA interface of a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

  Conditions: This symptom is observed when the router is configured for bridging across ATM IMA PVCs, when the PVCs carry traffic, and when a script runs that deletes and adds PVCs across the IMA links. These PVCs are not among the bridged PVCs that carry traffic. The router crashes in about one to two hours.

  Workaround: There is no workaround.

- CSCsb09190

  Symptoms: A router misses an entry in its label forwarding table, which is shown in the output of the **show tag-switching forwarding-table** EXEC command for the missing entry and in the output of the **show ip cef detail** EXEC command for the prefix.

  Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) and that learns its routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled.

  Workaround: There is no workaround. However, when you enter the **clear ip route** EXEC command for the affected prefix, the prefix is reinstalled in the label forwarding table.

- CSCuk49421

  Symptoms: A Cisco router that is running Cisco IOS Release 12.2, 12.2S, 12.2T, 12.3, or 12.3T may fail to fast switch IP packets correctly when NAT has been configured.

  Conditions: This problem can only occur when NAT has been configured on the router.

  Workaround: Disable fast-switching IP packets allow packets to be correctly process switched.

Wide-Area Networking

- CSCsa87205

  Symptoms: A router that is configured for PPP Multilink reloads because of a bus error.

  Conditions: This symptom is observed after a Telnet or SSH session is established when you enter the **who** command.

  Workarounds: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(29b)

Cisco IOS Release 12.2(29b) is a rebuild release for Cisco IOS Release 12.2(29). The caveats in this section are resolved in Cisco IOS Release 12.2(29b) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCeg62070

  Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

  Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

  Workaround: Disable HTTP server using the **no ip http server** command.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

- CSCse04560

  Symptoms: A tftp client trying to transfer a file from a Cisco IOS device configured as a tftp server and which is denied by an ACL receives a different result depending if the file is being offered for download or not. This may allow a third party to enumerate which files are available for download.

  Conditions: The **tftp-server** command is configured on the device and an ACL restricting access to the file in question has been applied as in this example:

```
tftp-server flash:filename1 access-list-number
access-list access-list- number
   permit 192.168.1.0 0.0.0.255
access-list access-list- number
   deny any
```

  Workaround: The following workarounds can be applied:

  1. Interface ACL Configure and attach an access list to every router interface active and configured for IP packet processing. Example:

```
access-list access-list- number
   remark --- the following hosts and networks area ALLOWED for TFTP access
access-list access-list- number
   permit udp host source_1
   host interface_address_1
   eq 69
access-list access-list- number
   permit udp host source_2
   host interface_address_2
   eq 69
access-list access-list- number
   permit udp source source- wildcard
   host interface_address_1
   eq 69
access-list access-list- number
   permit udp source source- wildcard
   host interface_address_2
   eq 69
access-list access-list- number
   remark --- everyone else is DENIED for TFTP access
access-list access-list- number
   deny udp any host interface_address_1
   eq 69
access-list access-list- number
   deny udp any host interface_address_2
   eq 69
access-list access-list- number
   remark --- any other traffic to/through the router is allowed
access-list access-list- number
   permit ip any any
```

```
   interface Ethernet0/0
   ip access-group access-list- number in
```

Once the tftp server in Cisco IOS is enabled and listening by default on all interfaces enabled for IP processing, the access list would need to deny traffic to each and every IP address assigned to any active router interface.

2. Control Plane Policing Configure and apply a CoPP policy. For example:

```
access-list access-list- number
   remark --- Do not police TFTP traffic from trusted hosts and networks
access-list access-list- number
   deny udp host source_1 any eq 69
access-list access-list- number
   deny udp source source- wildcard any eq 69
access-list access-list- number
   remark --- Police TFTP traffic from untrusted hosts and networks
access-list access-list- number
   permit udp any any eq 69
access-list access-list- number
   remark --- Do not police any other traffic going to the router
access-list access-list- number
   deny ip any any
class-map match-all tftp- class
   match access-group access-list- number
policy-map control-plane- policy
   ! Drop all traffic that matches the class tftp- class
   class tftp- class
      drop
control-plane service-policy input control- plane- policy
```

Note: CoPP is only available on certain platforms and Cisco IOS releases. Additional information on the configuration and use of the CoPP feature can be found at the following URL:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

3. Infrastructure ACLs (iACL) Although often difficult to block traffic transitting your network, identifying traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network is possible. Infrastructure 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 iACLs: http://www.cisco.com/warp/public/707/iacl.html

4. Configuring Receive Access Lists (rACLs) For distributed platforms, rACLs may be an option starting in Cisco IOS Release 12.0(21)S2 for the Cisco 12000 series GSR and Cisco IOS Release 12.0 (24)S for the Cisco 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path 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 CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled “GSR: Receive Access Control Lists” will help identify and allow legitimate traffic to your device and deny all unwanted packets: http://www.cisco.com/warp/public/707/racl.html

NOTE: The suggested workarounds are an “all or nothing” solution. While the tftp-server feature in Cisco IOS allows per-file ACLs to be attached to every file being offered for download, the suggested workarounds are global and will either prevent or allow access to all files being shared. It is recommended to apply the suggested workarounds in addition to the existing per-file ACLs, instead of replacing them.

- CSCsg70355

  Symptoms: Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

  Conditions: The Cisco IOS configuration command:

  clock summer-time *zone* **recurring**

  uses United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March. It changes the end date from the last Sunday of October to the first Sunday of November.

  Workaround: A workaround is possible by using the **clock summer- time** configuration command to manually configure the proper start date and end date for daylight savings time. After the summer-time period for calendar year 2006 is over, one can for example configure:

  clock summer-time *PDT* **recurring** *2 Sun Mar 2:00 1 Sun Nov 2:00*

  (This example is for the US/Pacific time zone.)

  Not A Workaround: Using NTP is not a workaround to this problem. NTP does not carry any information about timezones or summertime.

- CSCsj44081

  Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```
  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however, provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORRUPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCsi23231

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 (registered customers only) for non-12.2 mainline releases and CSCsi23231 (registered customers only) for 12.2 mainline releases.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsb26972

  Symptoms: A Cisco router may experience a bus error crash.

  Conditions: This symptom may be triggered by an event such as an ISDN connection.

  Workaround: There is no workaround.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- 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.

- CSCsj18014

  Symptoms: A caller ID may be received with extra characters.

  Conditions: This symptom is observed when caller ID is enabled on both routers and when the station ID and station name are configured on the FXS side.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at:
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  – The router must have RCP enabled.

  – The packet must come from the source address of the designated system configured to send RCP packets to the router.

  – The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

Resolved Caveats—Cisco IOS Release 12.2(29a)

Cisco IOS Release 12.2(29a) is a rebuild release for Cisco IOS Release 12.2(29). The caveats in this section are resolved in Cisco IOS Release 12.2(29a) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

Resolved Caveats—Cisco IOS Release 12.2(29)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(29). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(29). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCds33629

  Symptoms: Closing an existing Telnet session may cause a router to crash.

  Conditions: This symptom is platform-independent

  Workaround: There is no workaround.

- CSCeg64124

  Symptoms: The operation result of an IP SLA jitter probe shows a high packet MIA that is equal to the jitter's number of packets minus one. In the responder router, the responder debug message shows many error packets.

  Conditions: This symptom is observed when multiple jitter probes (either from the same router or from different routers) are configured to send packets to the same destination IP address and the same destination port number and when the responder is turned off for a short time and turned on again.

  Workaround: To prevent the symptom from occurring, configure the jitter probe to use a unique destination port number.

  Alternate Workaround: If the symptom has occurred, turn off the responder by entering the **no rtr responder** global configuration command, wait until all jitter probes report "No connection," and then turn on the responder by entering the **rtr responder** global configuration command.

- CSCeh34983

  Symptoms: A Cisco AS5400 gateway might stop unexpectedly, showing the following error message on the console:

  ```
  Breakpoint exception, CPU signal 23, PC = 0x603955C0
  ```

  Conditions: This symptom has been observed with Cisco IOS Release 12.2(27). This symptom has not seen on releases after Cisco IOS Release 12.2(4)T or on Cisco IOS Release 12.3 and later releases. This symptom has been seen only if an invalid attribute is configured in profile.

  Workaround: Configure all valid attributes in the profile.

DECnet

- CSCed88563

  Symptoms: On a Cisco Router, removing DecNet routing from the configuration can cause it to reload with a bus error.

  Conditions: This symptom has been observed when configuring more than one Tunnel interface, assigning decnet cost to them, and then removing the Tunnel interfaces. Subsequently if the decnet is unconfigured globally using the **no decnet routing** command, the router will reload with a bus error.

  Workaround: Remove the decnet cost configuration in the Tunnel interfaces before removing the Tunnel interfaces themselves.

IBM Connectivity

- CSCsa45750

  Symptoms: DLSw circuits are established over the same peer connection when there are multiple remote peer connections to the same remote MAC address.

  Conditions: This symptom is observed when DLSw load-balancing is configured and when there are multiple peers that have the **dlsw icanreach mac-address** *mac-addr* command enabled with the same remote MAC address for the *mac-addr* argument.

  Workaround: Bounce the DLSw peer connection either by entering the **dlsw disable** command or by removing and reconfiguring the DLSw remote peer statement.

  Further Problem Description: You can verify that the symptom occurs when the output of the **show dlsw reachability** command does not show the remote peer with the MAC address displayed as UNCONFIRMED or FOUND.

Interfaces and Bridging

- CSCeg73645

  Symptoms: A Versatile Interface Processor 2-50 (VIP2-50) crashes because of a Cybus error with DMA receive errors.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1 and that is configured with a PA-2FE that is installed in a VIP2-50. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCin86455

  Symptoms: Auto-provisioning may be disabled on a Cisco 7200 series that is configured with a PA-A3 port adapter.

  Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don’t Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef93215

  Symptoms: A router that is configured for OSPF may reload unexpectedly and reference the "ospf_build_one_paced_update" process.

  Conditions: This is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is very unlikely to occur. The symptom does not occur on a router that has exclusively stub areas and NSSA areas. The symptom may occur when a router does not have exclusively stub areas and NSSA areas.

- CSCsa51150

  Symptoms: When Network Address Translation (NAT) is configured, TCP translations do no time out properly when the TCP session is closed in a normal way.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 and that integrates the fix for CSCed93710. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed93710.

  Workaround: Lower the global NAT translation timeout period with the **ip nat translation tcp-timeout** *seconds* command.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Miscellaneous

- CSCeb07656

  Symptoms: There is no connectivity over an MLP link.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series that is configured with a FlexWAN in which a port adapter is installed. MLP is configured on an interface of the port adapter.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCeb60397

  Symptoms: A router crashes when you run the expValueCounter64Val object in the Expression MIB.

  Conditions: This symptom is observed on a Cisco router when the expObjectSampleType object is set to delta (2) in the expValueCounter64Val object.

  Workaround: There is no workaround.

- CSCec65977

  Symptoms: A 4-port serial enhanced port adapter (PA-4T+) may receive packets, even though the status of the serial interface is "down/down."

  Conditions: This symptom is observed on a PA-4T+ that is installed in a Cisco 7200 series router and that is connected to a 1-port serial WAN interface card (WIC-1T) that is installed in a Cisco 2600 series. The serial interfaces of both routers are connected with a CSU/DSU.

The input packet counter of the serial port of the PA-4T+ increments even though the status of the serial interface is "down/down." However, the 2600 series functions properly, and the input packet counter of its serial interface does not increment.

Possible Workaround: Administratively shut down the serial port.

- CSCed55201

  Symptoms: A serial interface may stop transmitting, and the following error message may be generated:

  ```
  %RSP-3-RESTART: interface Serial1/0/2, not transmitting
  -Traceback= 403D8D88 403E2830 4036B72C 4036B718
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an 8-port serial V.35 port adapter (PA-8T-V35).

  Workaround for HDLC interfaces: Disable CDP, the passive interface, and the outbound IP ACL.

  Workaround for Frame Relay interfaces: Disable CDP, the passive interface, the outbound IP ACL, and LMI.

- CSCee47441

  Symptoms: When the Cisco IOS Firewall CBAC is configured, the router seems to have a software-forced reload caused by one of the inspections processed.

  Conditions: This symptom is observed when the router is part of a DMVPN hub-spoke with a Cisco VoIP phone solution deployed on it and the router is connected to the central office over the Internet. The Cisco VoIP phone runs the SKINNY protocol.

  Workaround: There is no workaround.

- CSCef02332

  Symptoms: A Cisco 7200 series with high-speed serial interfaces such as HSSI interfaces or PA-2T3+ interfaces may reload unexpectedly.

  Conditions: This symptom is observed after you have performed an OIR of the HSSI or PA-2T3+ port adapter while traffic was being processed.

  Workaround: Stop the traffic while you perform the OIR or shut down the port adapter before you perform the OIR.

- CSCeg09274

  Symptoms: The line protocol of a serial interface of a PA-E3 may go down, and the output of the **show interfaces serial** *slot/port* command shows that the output queue is wedged (Output queue: 40/40) and that output drops increase.

  Conditions: This symptom is observed on a Cisco 7204VXR that is equipped with a PA-E3 when a Fast Ethernet interface is either shut down or disconnected and when the router is configured in the following way:

  – The **encapsulation frame-relay**, **frame-relay traffic-shaping**, and **tx-ring-limit** *ring-limit* commands are enabled on the serial interface of the PA-E3.

  – Multiple point-to-point subinterfaces with different Frame Relay Traffic Shaping (FRTS) parameters are applied on each of the subinterfaces, and Class Based Weighted Fair Queueing (CBWFQ) is applied on some of the subinterfaces.

  Workaround: Either enter the **shutdown** command followed by **no shutdown** command on the serial interface of the PA-E3 or enter the **clear interface serial** *slot/port* command on the serial interface of the PA-E3.

- CSCeg84558

  Symptoms: A Cisco 3745 reloads because of a bus error. Just before the crash, the following error messages are generated:

  ```
  %SYS-3-BAD_RESET: Questionable reset of process 149 on tty123
  %SYS-3-HARIKARI: Process Exec top-level routine exited
  ```

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.2(26) or Release 12.3(12) and that has an NM-2CE1T1-PRI network module that is configured for ISDN dial-in.

  Workaround: There is no workaround.

- CSCeh30146

  Symptoms: The WIC-DSU-T1-V2 card can get stuck and will not be able to detect any alarms, loopback events, etc.

  Conditions: When this symptom occurs, the DSU-T1-V2 may still be able to pass traffic.

  Workaround: Bring the card up again by issuing the **clear service- module serial** *slot|port* command.

- CSCeh71727

  Symptoms: The TCP Window size is changed after NAT translation.

  Conditions: This symptom is observed on a Cisco 7200 router with an NSE-1 processor board when PXF and NAT are enabled and TCP packets get forwarded.

  Workaround: Disable PXF globally by usign the **no ip pxf** command during configuration.

- CSCeh74304

  Symptoms: Packets going in and out of the same NAT inside interface are getting translated.

  Conditions: This symptom is observed on a Cisco 7200 with an NSE-1 processor board when PXF and NAT are enabled.

  Workaround: Disable PXF globally by using the **no ip pxf** command in the configuration.

- CSCin68688

  Symptoms: A Cisco 7200 series may reload unexpectedly when you perform an OIR of a PA-8T-V.35 serial port adapter. The tracebacks point to the mxt_periodic_processing routine.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1 and that processes a high load of AToM bidirectional traffic.

  Workaround: Shut down the serial interface before you perform the OIR.

- CSCsa55375

  Symptoms: A high error rate may occur on a WIC-1DSU-T1-V2. Because of the large number of errors, the interface of the WIC-1DSU-T1-V2 may not come up.

  Conditions: These symptoms are observed on a WIC-1-DSU-T1-V2 that is installed in a Cisco router.

  Possible Workaround: The symptoms may clear when you replace the in-house cabling with Cat.5 cables.

- CSCsa70703

  Symptoms: Memory leak at the Cisco gatekeeper causes the memory to constantly increase.

Conditions: This symptom has been observed on a Cisco gatekeeper running Cisco IOS Release 12.2(8)T1 or later. DGK leaks memory when sequential LRQ is configured and there is only one remote zone to forward LRQs to.

Workaround: There is no workaround.

Wide-Area Networking

- CSCec27865

  Symptoms: Packet forwarding may not function properly on a terminated Frame Relay permanent virtual circuit (PVC) that is configured on an ISDN link.

  Conditions: This symptom is observed on a Cisco 7200 series. The symptom does not occur on other platforms.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28d)

Cisco IOS Release 12.2(28d) is a rebuild release for Cisco IOS Release 12.2(28). The caveats in this section are resolved in Cisco IOS Release 12.2(28d) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCeg62070

  Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

  Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

  Workaround: Disable HTTP server using the **no ip http server** command.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

- CSCsj44081

  Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however, provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORRUPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of

network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- 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.

TCP/IP Host-Mode Services

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at:
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  – The router must have RCP enabled.

- The packet must come from the source address of the designated system configured to send RCP packets to the router.
- The packet must have a specific data content.

Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

Resolved Caveats—Cisco IOS Release 12.2(28c)

Cisco IOS Release 12.2(28c) is a rebuild release for Cisco IOS Release 12.2(28). The caveats in this section are resolved in Cisco IOS Release 12.2(28c) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCsb26972

  Symptoms: A Cisco router may experience a bus error crash.

  Conditions: This symptom may be triggered by an event such as an ISDN connection.

  Workaround: There is no workaround.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Resolved Caveats—Cisco IOS Release 12.2(28b)

Cisco IOS Release 12.2(28b) is a rebuild release for Cisco IOS Release 12.2(28). The caveats in this section are resolved in Cisco IOS Release 12.2(28b) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

Miscellaneous

- CSCsb09190

  Symptoms: A router misses an entry in its label forwarding table, which is shown in the output of the **show tag-switching forwarding-table** EXEC command for the missing entry and in the output of the **show ip cef detail** EXEC command for the prefix.

  Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) and that learns its routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled.

  Workaround: There is no workaround. However, when you enter the **clear ip route** EXEC command for the affected prefix, the prefix is reinstalled in the label forwarding table.

Resolved Caveats—Cisco IOS Release 12.2(28a)

Cisco IOS Release 12.2(28a) is a rebuild release for Cisco IOS Release 12.2(28). The caveats in this section are resolved in Cisco IOS Release 12.2(28a) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCsa81379

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing. The features are separate and distinct.

Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):

cnfFeatureAcceleration 1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable 1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot 1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot 1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable 1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry 1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType 1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot 1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive 1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches 1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches 1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges 1.3.6.1.4.1.9.9.99999.1.3.4.1.6

Resolved Caveats—Cisco IOS Release 12.2(28)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(28). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(28). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCee20816

  Symptoms: A system used for reverse connections, such as a console server or other “milking machine” applications, may unexpectedly restart due to a bus error.

  Conditions: The conditions under which this occurs are not well understood, but it is likely that frequent, short-lived connections are more likely to cause the problem than environments where connections are either long-lived or rarely opened and closed.

  Workaround: There is no workaround.

- CSCee84611

  Symptoms: An NTP broadcast client may fail to synchronize with an NTP broadcast server if the server cannot be reached from the client.

  Conditions: This symptom is observed in Cisco IOS interim Release 12.2(12.11)T or a later release, including Release 12.3. However, the symptom may also occur in other releases.

  Workaround: Ensure that the server can be reached from the client.

- CSCeg15044

  Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a “No Free TTYs error” message is generated.

  Conditions: This symptom is observed when there are simultaneous Telnet requests.

  Workaround: There is no workaround.

IBM Connectivity

- CSCef95672

  Symptoms: DLSw does not function when a SDLC station has the **sdlc role prim-xid-poll** command enabled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(10). The DLSw circuit is established, but the router does not send the XID to the SDLC station.

  Workaround: There is no workaround.

- CSCeg05690

  Symptoms: A software-forced crash may occur on a Cisco router that is configured with a Bisync Serial Tunnel (BSTUN).

  Conditions: This symptom is observed when line flaps occur on the asynchronous line that is attached to the BSTUN while the router attempts to forward packets via the asynchronous line.

  Workaround: Ensure that the asynchronous line does not flap.

Interfaces and Bridging

- CSCeg03185

  Symptoms: A few permanent virtual circuits (PVCs) go into a stuck state causing OutPktDrops on a Cisco 7200 router.

  Conditions: This symptom occurs on a Cisco 7200 router running Cisco IOS Release 12.2(26) with a PA-A3-T3 ATM interface. The symptom may also occur in other releases.

  Workaround: Remove and re-apply the PVC statement.

- CSCeg73645

  Symptoms: A Versatile Interface Processor 2-50 (VIP2-50) crashes because of a Cybus error with DMA receive errors.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1 and that is configured with a PA-2FE that is installed in a VIP2-50. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCin84694

  Symptoms: On a Cisco 7x00 series that runs Cisco IOS Release 12.3 and that is equipped with an ATM PA-A3 port adapter, the SAR chip of the port adapter may crash or the interface may become stuck.

Conditions: This symptom is observed when there is a high-traffic load on the ATM PA-A3 port adapter and when many VCs are created, deleted, and modified continuously. The symptom may also occur in other releases.

Workaround: There is no workaround.

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef93215

  Symptoms: A router that is configured for OSPF may reload unexpectedly and reference the "ospf_build_one_paced_update" process.

  Conditions: This is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is very unlikely to occur. The symptom does not occur on a router that has exclusively stub areas and NSSA areas. The symptom may occur when a router does not have exclusively stub areas and NSSA areas.

- CSCef97573

  Symptoms: A router may reload with a bus error exception, the crashinfo file shows an address error (a load or instruction fetch), and there is a spurious access in the crashinfo file.

  Conditions: These symptoms are observed on a Cisco router that performs NAT on H.323 voice traffic.

Workaround: There is no workaround.

- CSCsa51150

  Symptoms: When Network Address Translation (NAT) is configured, TCP translations do no time out properly when the TCP session is closed in a normal way.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 and that integrates the fix for CSCed93170. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed93170.

  Workaround: Lower the global NAT translation timeout period with the **ip nat translation tcp-timeout** *seconds* command.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

ISO CLNS

- CSCee83712

  Symptoms: A 60-second blackhole of an MPLS VPN flow (or any other flow to BGP) may occur when an IS-IS link fails or the metric of the IS-IS link is modified.

  Conditions: This symptom is observed on a Cisco platform that functions as a PE router and that is configured for BGP when the following conditions are present:

  - The PE performs loadbalancing to two links, which may be two links with the same metric to another router or two links to two different routers.
  - The **ip fast-convergence** command is enabled as part of the **router isis** command on the PE router.

Workaround: Disable the **ip fast-convergence** command. This workaround can only be applied if the platform is part of a network that does not target a 50-msec convergence time. If this is not an option, there is no workaround.

Miscellaneous

- CSCdz84448

  Symptoms: Spurious memory accesses may occur on a router, and the router may reboot.

  Conditions: This symptom is observed on a Cisco router when you poll the cbQosREDClassStatsTable of the CISCO-CLASS-BASED-QOS-MIB. The symptom is platform-independent. The spurious memory accesses may be reproduced when polling the above-mentioned table via Simple Network Management Protocol (SNMP).

  Workaround: Prevent the router from answering to queries on the cbQosREDClassStatsTable by implementing the following SNMP view in the router configuration:

  ```
  snmp-server view qos internet included
  snmp-server view qos 1.3.6.1.4.1.9.9.166.1.20.1 excluded
  snmp-server community string view qos ro
  ```

- CSCeb07656

  Symptoms: There is no connectivity over an MLP link.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series that is configured with a FlexWAN in which a port adapter is installed. MLP is configured on an interface of the port adapter.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCeb80992

  Symptoms: A router may reload unexpectedly because of a bus error when access control lists (ACL) counters are sent from a line card or network module to the Route Processor (RP).

  Conditions: This symptom is observed when the ACL number is in the expanded range (that is, from 1300 to 1999 or from 2000 to 2699). Note that the symptom does not occur when named ACLs are used.

  Workaround: There is no workaround.

- CSCed00033

  Symptoms: When an ATM PVC bounces, it fails to come back up and remains in the DOWN/UNVERIFIED state.

  Conditions: This symptom occurs when an ATM line card is connected to an ATM switch, when the ATM PVC is managed by OAM, and when the frequency of the OAM F5 loopback cells is set to 0 via the **oam-pvc manage 0** command.

  Workaround: Reactivate the PVC by entering the **shutdown** command followed by the **no shutdown** command on the PVC.

  Alternate Workaround: Disable OAM management.

- CSCed81317

  Symptoms: When an import map is configured on a VPN Routing/Forwarding (VRF) instance, the CE-learned routes are filtered out, preventing them from appearing in the VRF routing table.

Conditions: This symptom is observed when the **import map** *word* command is configured as part of the VRF configuration. Note that eBGP routes are not filtered out.

Workaround: There is no workaround.

- CSCee70591

  Symptoms: A Cisco 7500 series T3 port adapter (PA-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCef04072

  Symptoms: A learned RIP default route from a next hop router may not be removed from the routing table when the next hop router goes down.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.1 or Release 12.2 and occurs only when the router runs both EIGRP and RIP simultaneously. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef73120

  Symptoms: When you enter the **dsu bandwidth** *kbps* command, the router may not change the DSU bandwidth.

  Conditions: This symptom is observed on a Cisco router that is configured with an E3 serial port adapter.

  Workaround: There is no workaround.

- CSCeg00481

  Symptoms: A router fails to receive the Integrated Local Management Interface (ILMI) prefix from the switch side.

  Conditions: This symptom occurs during the initial negotiation of ILMI parameters. The output of **show atm ilmi-status** command does not show the configured ILMI prefix.

  Workaround: There is no workaround.

- CSCeg03153

  Symptoms: The ifAdminStatus MIB shows that subinterfaces are up when the main interface is shut down. This situation prevents SNMP from monitoring the proper status of the subinterfaces.

  Conditions: This symptom is observed when an ATM main interface is shut down but its subinterfaces are not.

  Workaround: Do not use the ifAdminStatus MIB. Rather, use the ifOperStatus MIB.

  Further Problem Description: The fix for this caveat ensures that when the main interface is shut down, the ifAdminStatus MIB does show that the subinterfaces are down too, whether or not the individual subinterfaces have been shut down.

- CSCeg16622

  Symptoms: A Cisco router that is configured for SNASw may reload because of a bus error.

  Conditions: This symptom is observed when the downstream port is configured for VDLC (DLSw). The symptom is platform-independent and is more likely to occur in a large, busy SNASw environment.

  Workaround: There is no workaround.

- CSCeg19008

  Symptoms: A PE router that is configured for MPLS may reload.

  Conditions: This symptom is observed when an MPLS adjacency is freed while the router performs label imposition on incoming IP packets.

  Workaround: There is no workaround.

- CSCeg23051

  Symptoms: A VIP may crash at “tagsw_flow_get”.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for egress NetFlow when any of the following events occur:

  – You toggle between the **ip cef distributed** global configuration command and the **ip cef** global configuration command.

  – You enter the **clear cef linecard** EXEC command.

  – You toggle between the **tag-switching ip** global configuration or interface configuration command and the **no tag-switching ip** global configuration or interface configuration command.

  – You toggle between the **mpls netflow egress** interface configuration command and the **no mpls netflow egress** interface configuration command.

  If a VIP in one slot crashes, another VIP in another slot may crash because of caveat CSCeg23051 or caveats CSCdx14343.

  Workaround: There is no workaround.

- CSCin83377

  Symptoms: After a router reloads, a permanent virtual circuit (PVC) configuration may be lost from a virtual circuit (VC).

  Conditions: The symptom is observed on a Cisco 7xxx series router when the VC is configured under an IMA-group interface of a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

  Workaround: Save the configuration to disk or in bootflash. After the router has reloaded and come up, copy the configuration from the disk or bootflash to the running configuration.

Wide-Area Networking

- CSCsa49019

  Symptoms: A memory leak may occur in the "Multilink Events" process, which can be seen in the output of the **show memory summary** command:

```
0x60BC47D0 0000000024 0000000157 0000003768    MLP bundle name
0x60BC47D0 0000000028 0000000003 0000000084    MLP bundle name
0x60BC47D0 0000000044 0000000001 0000000044    MLP bundle name
0x60BC47D0 0000000048 0000000001 0000000048    MLP bundle name
0x60BC47D0 0000000060 0000000001 0000000060    MLP bundle name
0x60BC47D0 0000000064 0000000013 0000000832    MLP bundle name
0x60BC47D0 0000000068 0000000008 0000000544    MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072    MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076    MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584    MLP bundle name
```

  Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(27c)

Cisco IOS Release 12.2(27c) is a rebuild release for Cisco IOS Release 12.2(27). The caveats in this section are resolved in Cisco IOS Release 12.2(27c) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCeg62070

  Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

  Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

Workaround: Disable HTTP server using the **no ip http server** command.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

- CSCsj44081

  Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```
  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however, provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORRUPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCeb21064

  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

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsc60249

  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

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  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

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- 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.

- 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

- 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

- CSCse68138

  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

TCP/IP Host-Mode Services

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at:
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  – The router must have RCP enabled.

  – The packet must come from the source address of the designated system configured to send RCP packets to the router.

  – The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

Resolved Caveats—Cisco IOS Release 12.2(27b)

Cisco IOS Release 12.2(27b) is a rebuild release for Cisco IOS Release 12.2(27). The caveats in this section are resolved in Cisco IOS Release 12.2(27b) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

Miscellaneous

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Resolved Caveats—Cisco IOS Release 12.2(27a)

Cisco IOS Release 12.2(27a) is a rebuild release for Cisco IOS Release 12.2(27). The caveats in this section are resolved in Cisco IOS Release 12.2(27a) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages

2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages

  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Miscellaneous

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Resolved Caveats—Cisco IOS Release 12.2(27)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(27). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(27). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCed86286

  Symptoms: A router may reload due to a software-forced crash.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.2(13)T5 and that has SSH configured. However, the symptom may occur on other platforms that run other releases and that do not have SSH configured.

  Workaround: There is no workaround.

- CSCee20816

  Symptoms: A system used for reverse connections, such as a console server or other “milking machine” applications, may unexpectedly restart due to a bus error.

  Conditions: The conditions under which this occurs are not well understood, but it is likely that frequent, short-lived connections are more likely to cause the problem than environments where connections are either long-lived or rarely opened and closed.

  Workaround: There is no workaround.

- CSCee35740

  Symptoms: After a VIP crashes, a FIB-3-FIBDISABLE error message due to an IPC timeout may occur for all the slots of the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series after the VIP crashes and before the VIP recovers. The FIB-3-FIBDISABLE error message is generated for all the slots of the VIP, causing dCEF switching to become disabled.

  Workaround: There is no workaround. You can reenable dCEF by entering the **clear cef linecard** command.

- CSCee84611

  Symptoms: An NTP broadcast client may fail to synchronize with an NTP broadcast server if the server cannot be reached from the client.

  Conditions: This symptom is observed in Cisco IOS interim Release 12.2(12.11)T or a later release, including Release 12.3. However, the symptom may also occur in other releases.

  Workaround: Ensure that the server can be reached from the client.

- CSCef26714

  Symptoms: The Route Switch Module (RSM) fails to boot up and is not listed as a valid module.

  Conditions: This symptom happens with Cisco IOS Release 12.2(26) only.

  Workaround: Use an older or a newer image than Cisco IOS Release 12.2(26).

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

Interfaces and Bridging

- CSCee44827

  Symptoms: Spurious memory accesses may occur on a VIP with a PA-FE.

Conditions: This symptom is observed on a Cisco 7500 series when a raw Ethernet packet is received on the PA-FE interface that is configured as an ISL trunk.

Workaround: There is no workaround.

- CSCin58433

  Symptoms: The driver code of a third-party vendor Fast Ethernet controller that is part of a C7200-I/O-FE I/O controller may pause indefinitely or reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series when a packet enters the third-party vendor Fast Ethernet controller, when this packet is forwarded to a Multilink PPP (MLP) interface, and when another packet is forwarded by the third-party vendor Fast Ethernet controller before the first packet has left the MLP interface.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed53358

  Symptoms: Pings fail on an Ethernet-to-VLAN interworking over L2TPv3 due to an IRDP failure.

  Conditions: This symptom is observed when you ping between two CE routers. Both of the CE routers do not learn each other's MAC address automatically.

  Workaround: Ping from the first CE router to the second CE router, then ping from the second CE router to the first CE router.

- CSCee32675

  Symptoms: It may not be possible to remove a VRF-based static NAT configuration.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 in an MPLS VRF NAT configuration.

  Workaround: There is no workaround.

- CSCee35125

  Symptoms: A Cisco router may crash when you enter the **clear ip route *** command.

  Conditions: This symptom is observed when the routing table has a default route.

  Workaround: There is no workaround.

- CSCee66936

  Symptoms: A software-forced reload may occur on a router that is configured with a DVMRP tunnel.

  Conditions: This symptom is observed on a Cisco router when the DVMRP tunnel is brought up and routing information is redistributed between DVMRP and MBGP.

  Workaround: There is no workaround.

Miscellaneous

- CSCdt59350

  Symptoms: X.25 encapsulation may not work on interfaces of a Fast Ethernet network module (NM-xFE2W).

Conditions: This symptom is observed when the NM-xFE2W is installed in a Multicast Address Resolution Server (MARS) platform.

Workaround: There is no workaround.

- CSCdz74292

  Symptoms: T.38 fax calls from one gateway to another gateway may fail.

  Conditions: This symptom is observed when you make a T.38 fax call from an originating gateway (OGW) that is running Cisco IOS Release 12.2(13)T and that is configured for H.323 fast start mode through a gatekeeper to a gateway that is running Cisco IOS Release 12.2(11)T2.

  Workaround: Configure the **voice service voip** global configuration command followed by the **h323 call start slow** voice-service configuration command on the OGW.

- CSCdz84448

  Symptoms: When polling the cbQosREDClassStatsTable of the CISCO-CLASS-BASED-QOS-MIB, spurious memory accesses may occur on a Cisco 2600 series, Cisco 3600 series, or Cisco 7200 series. A Cisco 3640 router may also reboot. The spurious memory accesses may be reproduced when polling the above-mentioned table via Simple Network Management Protocol (SNMP).

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series that run Cisco IOS Release 12.2(8)T, Release 12.3, or Release 12.3 T.

  Workaround: Prevent the router from answering to queries on the cbQosREDClassStatsTable by implementing the following SNMP view in the router configuration:

  snmp-server view qos internet included

  snmp-server view qos 1.3.6.1.4.1.9.9.166.1.20.1 excluded

  snmp-server community *string* **view qos ro**

- CSCdz90367

  Symptoms: A CPUHOG condition may occur on a router, and the router may reload.

  Conditions: This symptom is observed when the router has a large configuration that contains several static crypto map statements and associated crypto access control lists (ACLs).

  Workaround: Reduce the size of the configuration, which may help alleviate the CPUHOG condition and reduce the likelihood that the router may reload.

- CSCea26450

  Symptoms: Under rare circumstances, an Operation, Administration, and Maintenance (OAM)-enabled ATM Permanent Virtual Circuit (PVC) may stay in the down state.

  Conditions: This symptom is observed when the ATM interface transitions to the down state and then back to the up state because of a-link related problem or because you enter the **shutdown** command followed by the **no shutdown** command.

  Workaround: Disable OAM on the PVC.

- CSCea87364

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled on a Versatile Interface Processor (VIP) or Cisco 12000 series line card (LC), and the following error message may appear on the console:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 12: Window did not open, LC to RP IPC is
  non-operational
  ```

Conditions: This symptom is observed on a Cisco 7500 series VIP2-50 and VIP4- 80 in which ATM OC-3 port adapters such as the PA-A1-OC3 or PA-A3-OC3 are installed when the Cisco 7500 series is upgraded to Cisco IOS Release 12.0(24) S or Release 12.0(24)S1. This symptom is also observed on a Cisco 12000 series LC during significant, prolonged routing table churn.

Workaround: Reload CEF on the VIP or LC by entering the **clear cef linecard** *slot-number* EXEC command.

Alternate Workaround: Restart the VIP by performing an online insertion and removal (OIR). Restart the LC by executing the **hw-module slot** *slot #* **reload** command.

- CSCeb01205

  Symptoms: CPUHOG and Switch1 bad VCD error with traceback is observed on a router configured as a PE router.

  ```
  May 5 16:50:22.637: %SYS-3-CPUHOG: Task ran for 2816 msec (348/345), process = Virtual
  Exec, PC = 600EEA30. -Traceback= 600EEA38 600776C0 60078564 603146F0 602DD204 602DD2BC
  602C9FCC 602DCD48 60353F0C 60353EF0

  May 5 16:50:32.441: %ATMPA-3-BADVCD: Switch1 bad vcd 3137 packet - 0C418847 00052C3B
  00B3DD3B 456B012C 00000000 3B008B0E
  ```

  Conditions: Upon execution of the **clear interface sw1** command, %ATMPA-3-BADVCD Switch1 BADVCD with traceback error is observed. The setup has approximately 800 LVCs and 1000 PVCs. This issue is reproducible on platforms which exceed a CPU cycle of more than 2 seconds for 100 VCs.

  Workaround: There is no workaround.

- CSCeb52181

  Symptoms: A Cisco platform that accesses the “system:/vfiles/tmstats_ascii” virtual file (for example, via “more system:/vfiles/tmstats_ascii”) may crash because of bus error.

  Conditions: This symptom is observed under normal working conditions when no configuration changes are made on a Cisco platform that runs Cisco IOS Release 12.0 S, 12.1 E, 12.2 or 12.3. When the “system:/vfiles/tmstats_ascii” virtual file is not used, the symptom does not occur.

  Workaround: There is no workaround.

- CSCed49294

  Symptoms: A Cisco 3600 series with an NM-CT1/E1 network module that contains an NM-xDM network module may not allow incoming modem calls and generate the “no modem available” error message even though the output of the **show modem** command indicates that there is a free modem available.

  Conditions: This symptom is observed when frequent retrains occur on the modems.

  Workaround: There is no workaround.

- CSCee14926

  Symptom: The PE router configured with MPLS may reload due to freed mpls adjacency while doing label imposition on the received IP packets.

  Conditions: The condition is label imposition to the received packets on the PE router configured with MPLS.

  Workaround: There is no workaround.

- CSCee22810

  Symptoms: On a Cisco 7500 series, all PVCs may suddenly enter the down state and remain in this state for about two minutes before they come back up. During the DLCI down state, the subinterface does not go down and no notifications are observed in the message log.

Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RPS4+ or an RSP8 and that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(12i). In addition, the router is configured with an 8-port serial port adapter and an HSSI port adapter, is configured for Frame Relay, and has more than 450 PVCs/DLCIs. Note that the symptom may be platform-independent and may also occur on other Cisco platforms in a similar configuration.

Workaround: There is no workaround.

- CSCee23750

  Symptoms: When you enter the **format flash:** command on a router to format a LEFS flash card, the router fails to give the DOS format and displays this error:

  ```
  %Error formatting flash (Invalid DOS media or no media in slot)
  The flash card is no longer accessible until the router is reloaded.
  ```

  Conditions: This symptom is observed on any Cisco router that supports a disk file system and that runs Cisco IOS Release 12.3(6) or a later release. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee53709

  Symptoms: A Cisco 3700 series with an NM-1A-OC3, NM-1A-T3, or NM-1A-E3 network module with many VCs of the same class may reload because of a bus error.

  Conditions: This symptom is observed when you configure more than 255 VCs of the same QoS type on the ATM interface, when traffic is processed on all VCs, and when a line error occurs.

  Workaround: There is no workaround.

- CSCee56098

  Symptoms: After running traffic for 24 to 36 hours on an ATM subinterface, tracebacks occur, and the ATM interface and all ATM subinterfaces on the same network module stop sending traffic although the ATM interface is still in the “up/up” state. A ping fails on the interface and the EIGRP neighbor may also be lost. OAM functionality is not affected.

  The ATM SAR reports many CRC errors, length violations, and timeout errors. The framer does not report any physical level problems.

  Conditions: These symptoms are observed on a Cisco 2600 series that is configured with an ATM network module after running traffic for 24 to 36 hours on the ATM subinterface.

  Temporary Workaround: Reset the router until the symptoms occur again after 24 to 36 hours.

- CSCee74111

  Symptoms: A Cisco voice gateway may reload with a bus error at an invalid address and generate the following error message:

  System was restarted by bus error at by bus error at PC 0x60C7D834, address 0xD0D0D23

  Conditions: This symptom is observed on a Cisco voice gateway that runs Cisco IOS Release 12.2(23b) and that is configured for H.323. The symptom may also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCee79728

  Symptoms: A router running Cisco IOS Release 12.2(13b)M2 may crash with a Bus Error exception.

  Conditions: This symptom is observed on routers running Cisco IOS Release 12.2 (13b)M2.

  Workaround: Problem seems to be in the process switching path, so enabling the **ip route cache** command on all interfaces should help.

- CSCee80885

  Symptoms: A Cisco voice gateway may reload with a bus error at an invalid address:

  System was restarted by bus error at PC 0x60C5BD30, address 0xD391832C

  Conditions: This symptom is observed on a Cisco voice gateway that is running Cisco IOS Release 12.2(23b) and H.323.

  Workaround: There is no workaround.

- CSCee82681

  Symptoms: On an RTR probe, an RSP does not report input or output packets for serial interfaces of PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(23a) or Release 12.3 and is more likely to occur when the number of channelized port adapters (such as the PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters) that are installed in the router is high. The symptom may also occur in other releases.

  Workaround: Reload the router.

  Alternate Workaround: Enter the **reload microcode** router configuration command.

- CSCee88793

  Symptoms: An HPR/RTP connection, identified by a TCID, may perform very slowly because of an excessively large delay change sum (DCS) value.

  Conditions: This symptom is observed when a Cisco platform that functions as an HPR endpoint performs a path switch in times of instability. The DCS of the router may become corrupted because of the incorrect calculation of the last received rate request.

  Workaround: Initiate a manual path switch at the mainframe end to reset the connection and clear the condition. Otherwise, reset the TCID, or wait until the natural decay of the DCS returns it to zero.

- CSCef14999

  Symptoms: IP SNMP CPU utilization increases to 99 percent when you query for SNASw and DLSw via the mib-2.34.4.1 OID. The CPU utilization of the router goes to 99 percent with about 75 percent in use by the SNASw process.

  When you stop the snmpwalk, process, the CPU utilization of the router remains high, and SNASw functionality is affected. When you enter the **snasw stop** command followed by the **snasw start** command, SNASw functionality is restored but after you enter the **snasw stop** command, error messages similar to the following ones are generated:

  ```
  %SNASW-3-MIBQueryFailure: Query Mode failed. NOF primary rc=4F0 secondary rc=0.
  %SNASW-3-MIBQueryFailure: Query COS failed. NOF primary rc=4F0 secondary rc=0.
  %SNASW-3-MIBQueryFailure: Query COS Node Row failed. NOF primary rc=4F0 secondary
  rc=0.
  %SNASW-3-MIBQueryFailure: Query COS Node Row failed. NOF primary rc=4F0 secondary
  rc=0.
  %SNASW-3-MIBQueryFailure: Query COS Node Row failed. NOF primary rc=4F0 secondary
  rc=0.
  %SNASW-3-MIBQueryFailure: Query COS Node Row failed. NOF primary rc=4F0 secondary
  rc=0.
  %SNASW-3-MIBQueryFailure: Query COS Node Row failed. NOF primary rc=4F0 secondary
  rc=0.
  %SNASW-3-MIBQueryFailure: Query COS TG Row failed. NOF primary rc=4F0
  ```

  Conditions: These symptoms are observed on a Cisco 7204VXR that runs Cisco IOS Release 12.3.(9) but could occur on any platform that is configured for SNASw.

Workaround: Stop all DLUR LU-LU sessions, or stop SNASwitch completely.

- CSCef16997

  Symptom: An I/O memory leak occurs when BSTUN is configured; an interrupt without any data is received.

  Conditions: This symptom is observed on a Cisco 2600 series that is configured with a WIC-2A/S.

  Workaround: There is no workaround.

- CSCef44225

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef58120

  Symptoms: A DLC trace shows that SNASw includes an illegal TG vector in a Topology Update flow to a DLUS host. The TG vector contains a TG that both originates and terminates at the local SNASw node. The host log may show this rejection with sense code 10010021.

  Conditions: This symptom is observed when a DLUR-DLUS session is started with the host. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz25898. 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. However, there is no harmful impact so the symptoms may be ignored.

- CSCef58292

  Symptoms: A Snasw router may crash and reload.

  Conditions: This symptom is observed when the Snasw router has enterprise extender connections configured to multiple upstream main frames and one of the main frames is IPLed.

  Workaround: There is no workaround.

- CSCef70606

  Symptoms: A Cisco 2651 router with a WIC-2T installed running Cisco IOS Release 12.2(26.8) will have a problem if trying to configure a serial interface for anything other than HDLC.

  When configuring encapsulation frame-relay on a serial interface, the command appears to be accepted. However, the interface remains HDLC, as seen in **show interface** and **show run** commands, and does not reflect encapsulation frame-relay. When configuring bstun, the same situation arises. When configuring ppp, the interface changes encapsulation to ppp, but it cannot be changed back.

  Conditions: This symptom was observed on a Cisco 2651 router with a WIC-2T installed running Cisco IOS Release 12.2(26.8). This symptom may occur on other platforms or interface types but definitely is seen on serial interfaces.

  Workaround: There is no workaround.

- CSCin38132

  Symptom: A Cisco 7xxx series may crash.

  Conditions: This symptom is observed when the traffic rate via a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter is very high (at about or higher than the line rate).

  Workaround: There is no workaround.

- CSCin67741

  Symptoms: The Route Processor (RP) crashes when encapsulation is removed using the **no encapsulation** command.

  Conditions: This symptom has been observed on a multilink interface with DLFI configuration under traffic.

  Workaround: There is no workaround.

- CSCin68712

  Symptoms: A Cisco 7500 series router may reload when multilink interface configured on the router comes up.

  Conditions: This symptom would happen if service-policy is configured on the multilink interface and distributed switching is enabled.

  Workaround: Not configuring service-policy on the router would prevent the router from reloading.

- CSCin83377

  Symptoms: After reload, the loss of permanent virtual circuit (PVC) configuration can happen on virtual circuits (VC) which are configured under the IMA-group interface of PA-A3-8T1IMA/PA-A3-8E1 IMA PA on Cisco 7xxx series routers.

  Conditions: The problem happens on the IMA-group interface of PA-A3-8T1IMA/PA- A3-8E1 IMA PA on Cisco 7xxx series routers.

  Workaround: Save the configuration to disk or in bootflash. After the reload and the router comes up, copy the configuration from the disk or bootflash to the running configuration.

- CSCuk44685

  Symptoms: If an online insertion and removal (OIR) occurs on the slot of a line card with interprocess communications (IPC) traffic running, the forwarding information base (FIB) on the other slots or on a secondary route processor (RP) may be disabled.

  The following error messages are logged on the router:

  ```
  %OIR-6-REMCARD: Card removed from slot 0, interfaces disabled
  ```

```
%HA-5-SYNC_NOTICE: OIR sync started.
%HA-5-SYNC_NOTICE: OIR sync completed.
%OIR-6-INSCARD: Card inserted in slot 0, interfaces administratively s hut down
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
(1/1),process = OIR Handler.
-Traceback= 4043F544 404D667C 404D7698 404EEB94 404E01B4
%SYS-3-CPUHOG: Task is running for (4000)msecs, more than (2000)msecs
(1/1),process = OIR Handler.
-Traceback= 404D6680 404D7698 404EEB94 404E01B4
%SYS-3-CPUHOG: Task is running for (6000)msecs, more than (2000)msecs
(1/1),process = OIR Handler.
-Traceback= 4043F56C 404D667C 404D7698 404EEB94 404E01B4
%SYS-3-CPUHOG: Task is running for (8000)msecs, more than (2000)msecs
(1/1),process = OIR Handler.
-Traceback= 404D6680 404D7698 404EEB94 404E01B4
%HA-5-SYNC_NOTICE: OIR sync started.
%FIB-3-FIBDISABLE: Fatal error, slot/cpu 2/0: IPC Failure: timeout <<<<<<<<<< !!!!
```

Conditions: This symptom is observed on a Cisco Route Switch Processor (RSP) router that is running Cisco IOS software.

Workaround: There is no workaround. The FIB may be reenabled by entering the **no ip cef distributed** global configuration command followed by the **ip cef distributed** global configuration command.

- CSCuk51269

  Symptoms: Multicast packets such as HSRP and OSPF are not received on a port-channel interface.

  Conditions: This symptom is observed when a port-channel interface is configured on a Cisco router, when you reload the router, and when the first member is added to the port-channel interface by entering the **no shutdown** interface configuration command on physical interface.

  Workaround: Enter the do **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port-channel interface.

- CSCuk51673

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled and the following error message may appear on the console:

  ```
  %FIB-3-NOMEM: Malloc Failure, disabling DCEF %FIB-2-FIBDOWN: CEF has been disabled
  due to a low memory condition. It can be re-enabled by configuring "ip cef
  [distributed]"
  ```

  Conditions: This may be seen on a platform running DCEF. DCEF may get disabled. This depends on how much memory is being allocated at runtime.

  Workaround: Upgrade to the image containing this bug-fix.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Wide-Area Networking

- CSCed78803

  Symptoms: A Cisco router may forward packets that come in on a subinterface that is in an administratively shut down state.

  Conditions: This symptom is observed on a Cisco router that is configured with Frame Relay encapsulation.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(26c)

Cisco IOS Release 12.2(26c) is a rebuild release for Cisco IOS Release 12.2(26). The caveats in this section are resolved in Cisco IOS Release 12.2(26c) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCeg62070

  Symptoms: Tracebacks or crash are seen during HTTP transactions with long URLs.

  Conditions: The crash is seen when the length of any token in the URL of the request is excessively long.

  Workaround: Disable HTTP server using the **no ip http server** command.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

- CSCsj44081

  Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```
  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however, provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORRUPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

IP Routing Protocols

- CSCec71950

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability.

  This vulnerability was discovered during internal testing.

  This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Miscellaneous

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml

Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCeb21064

  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

- CSCsc60249

  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

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  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

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml.

- CSCse68138

  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

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- 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.

- 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

- 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

TCP/IP Host-Mode Services

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177

  There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at:
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  - The router must have RCP enabled.
  - The packet must come from the source address of the designated system configured to send RCP packets to the router.
  - The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

Resolved Caveats—Cisco IOS Release 12.2(26b)

Cisco IOS Release 12.2(26b) is a rebuild release for Cisco IOS Release 12.2(26). The caveats in this section are resolved in Cisco IOS Release 12.2(26b) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

Miscellaneous

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Resolved Caveats—Cisco IOS Release 12.2(26a)

Cisco IOS Release 12.2(26a) is a rebuild release for Cisco IOS Release 12.2(26). The caveats in this section are resolved in Cisco IOS Release 12.2(26a) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Miscellaneous

- CSCea87364

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled on a Versatile Interface Processor (VIP) or Cisco 12000 series line card (LC), and the following error message may appear on the console:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 12: Window did not open, LC to RP IPC is
  non-operational
  ```

  Conditions: This symptom is observed on a Cisco 7500 series VIP2-50 and VIP4- 80 in which ATM OC-3 port adapters such as the PA-A1-OC3 or PA-A3-OC3 are installed when the Cisco 7500 series is upgraded to Cisco IOS Release 12.0(24) S or Release 12.0(24)S1. This symptom is also observed on a Cisco 12000 series LC during significant, prolonged routing table churn.

  Workaround: Reload CEF on the VIP or LC by entering the **clear cef linecard** *slot-number* EXEC command.

  Alternate Workaround: Restart the VIP by performing an online insertion and removal (OIR). Restart the LC by executing the **hw-module slot** *slot #* **reload** command.

- CSCee22810

  Symptoms: On a Cisco 7500 series, all PVCs may suddenly enter the down state and remain in this state for about two minutes before they come back up. During the DLCI down state, the subinterface does not go down and no notifications are observed in the message log.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RPS4+ or an RSP8 and that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(12i). In addition, the router is configured with an 8-port serial port adapter and an HSSI port adapter, is configured for Frame Relay, and has more than 450 PVCs/DLCIs. Note that the symptom may be platform-independent and may also occur on other Cisco platforms in a similar configuration.

  Note. This is a timing issue and is not dependant on the number of VC's.

  Workaround: There is no workaround.

- CSCee80885

  Symptoms: A Cisco voice gateway may reload with a bus error at an invalid address:

  System was restarted by bus error at PC 0x60C5BD30, address 0xD391832C

  Conditions: This symptom is observed on a Cisco voice gateway that is running Cisco IOS Release 12.2(23b) and H.323.

  Workaround: There is no workaround.

- CSCef44225

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

Resolved Caveats—Cisco IOS Release 12.2(26)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(26). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(26). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust

resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In UserService (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

- CSCed67358

  Symptoms: An IPv6 PIM neighbor may be down after changing the PIM configuration.

  Conditions: This symptom is observed when the **no ipv6 pim** command is entered on some subinterfaces of a physical Ethernet interface and PIM is enabled on several subinterfaces of the same physical Ethernet interface.

  It affects both IPv4 and IPv6, for multicast and OSPF Hello message.

  Workaround: There is no workaround.

- CSCee42381

  Symptoms: A Cisco MC3810 reloads when you configure ILMI on an ATM interface.

  Conditions: This symptom is observed on a Cisco MC3810 that runs Cisco IOS Release 12.3(9).

  Workaround: There is no workaround.

IBM Connectivity

- CSCed77877

  Symptom: A 4-port serial enhanced port adapter (PA-4T+) may not function when the Synchronous Data Link Control (SDLC) protocol is configured.

  Conditions: This symptom is observed on a Cisco 7200.

  Workaround: Reload the router to re-initialize the role used in the previous connection.

- CSCee40967

  Symptoms: A Cisco router may crash due to a bus error if a PA-A1-OC3MM ATM port adapter is installed but not configured for ATM LANE.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(8.4a), which is an interim release for Release 12.3(9).

  Workaround: There is no workaround.

- CSCin76076

  Symptoms: A Cisco router that functions as a LANE server may fail to attain the active state and remains in the backup state regardless of the priority. This situation prevents LANE clients from becoming operational.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that run Cisco IOS interim Release 12.3(8.4) and later interim releases. The symptom may also occur in other releases.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCeb59227

  Symptoms: The ifOutUcastPkts, ifOutOctets, and ifHCOutOctets Simple Network Management Protocol (SNMP) counters of a Fast Ethernet subinterface may not be incremented.

  Conditions: This symptom is observed on a Cisco 7500 series when traffic is received from a serial interface in a Multiprotocol Label Switching (MPLS) network and when the Fast Ethernet subinterface is configured for dot1q encapsulation.

  Workaround: There is no workaround.

- CSCeb81473

  Symptoms: A Cisco 7500 series that is configured as a bridge may not pass bridged traffic on a FDDI interface. This situation may lead to a loss of connectivity.

  Conditions: This symptom is observed on Cisco 7500 series that runs a Cisco IOS rsp-jsv-mz image.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the FDDI interface.

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

  Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP).

  Workaround: There is no workaround.

- CSCee44827

  Symptoms: Spurious memory accesses may occur on a VIP with a PA-FE.

  Conditions: This symptom is observed on a Cisco 7500 series when a raw Ethernet packet is received on the PA-FE interface that is configured as an ISL trunk.

  Workaround: There is no workaround.

- CSCin58433

  Symptoms: The driver code of a third-party vendor Fast Ethernet controller that is part of a C7200-I/O-FE I/O controller may pause indefinitely or reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series when a packet enters the third-party vendor Fast Ethernet controller, when this packet is forwarded to a Multilink PPP (MLP) interface, and when another packet is forwarded by the third-party vendor Fast Ethernet controller before the first packet has left the MLP interface.

  Workaround: There is no workaround.

- CSCin67296

  Symptoms: Channelized interfaces on a channelized T3 line card or port adapter that is configured for Frame Relay encapsulation may be in the up/down state, and DLCIs are inactive.

  Conditions: This symptom is observed when you reload a Cisco platform and when the interfaces were in the up/up state before you reloaded the platform.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller of either the T3 line card or port adapter on the Cisco platform or on the T3 line card or port adapter on the platform at the remote end.

Alternate Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the main interface on the Cisco platform.

IP Routing Protocols

- CSCeb17467

  Symptoms: A Cisco router may reload when Border Gateway Protocol (BGP) is configured to carry Virtual Private Network version 4 (VPNv4) routes.

  Conditions: This symptom is observed when VPNv4 import processing occurs simultaneously with a BGP neighbor reset, for example, when a VPN routing and forwarding (VRF) instance is configured and you enter the **clear ip bgp *** privileged EXEC command.

  Workaround: There is no workaround.

- CSCed33044

  Symptoms: ARP may not function properly on the remote side of point-to-point Fast Ethernet link with a default static route until the remote side is pinged.

  Conditions: This symptom is observed on a Cisco router when ARP and /31 mask are configured on a point-to-point link Fast Ethernet link with a default static route. The symptom is platform-independent.

  Workaround: There are four different workarounds:

  - Use a /30 netmask on the point-to-point Fast Ethernet connection.

  - Configure a static ARP entry for the remote side of the Fast Ethernet link.

  - Enter the **ip proxy-arp** command on the remote side of the Fast Ethernet link.

  - Use an OSPF route instead of a default static route.

- CSCed93710

  Symptoms: NAT is causing some TCP packets to be punted up to process switching. This causes those process switched packets to go through the router slower than the rest of the TCP packets that go through in the fast path. These out-of-order packets are causing this stream to be stopped by the firewall because the firewall thinks these are SYN attack packets instead of a valid TCP stream.

  Conditions: If there is enough latency in the Internet then there will be a big enough gap between the packets not to cause this problem. But if you have a fast connection to the Internet this timing issue could arise.

  Workaround: Either disable NAT or disable CEF and the **ip route-cache** command.

- CSCee66936

  Symptoms: A software-forced reload may occur on a router that is configured with a DVMRP tunnel.

  Conditions: This symptom is observed on a Cisco router when the DVMRP tunnel is brought up and routing information is redistributed between DVMRP and MBGP.

  Workaround: There is no workaround.

Miscellaneous

- CSCdt38401

  Symptoms: Cisco Express Forwarding (CEF) believes a interface is down when it is in fact up, which causes CEF forwarding not to work for traffic destined to this interface.

  Conditions: This symptom occurs during rapid interface flaps.

  Workaround: Shut the interface down and bring the interface back up again.

- CSCdy47578

  Symptoms: A router may reload when a turbo access list that is referred to in a route map is created.

  Conditions: This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.2(10a). This symptom is observed only when turbo access lists are used.

  Workaround: Disable the turbo access list by entering the **no access-list compiled** global configuration command.

- CSCdy55352

  Symptoms: N flag gets incorrectly set on the mroute entry of the Line Card causing high data rate packets to get punted and then spd dropped.

  Conditions: Occurs when high data rate packets are sent.

  Workaround: First send few packets so that the N flag gets reset.

- CSCeb85255

  Symptoms: A unexpected reload can occur on a Cisco 1000 series and Cisco 6400 series with an ATM interface.

  Conditions: When executing the **show atm** command.

  Workaround: There is no workaround.

- CSCec03907

  Symptoms: A Route Switch Processor 4 Plus (RSP4+) may reload.

  Conditions: This symptom is observed on a Cisco 7500 series when you configure the **interface loopback** *interface-number* interface configuration command on an interface of the router and the value of the *interface-number* argument is a 9-digit number that starts with 10.

  Workaround: If possible, use another range of numbers for the numbers that are assigned to the loopback interfaces, that is, a range of numbers that do not start with 10.

- CSCed49294

  Symptoms: A Cisco 3600 series with an NM-CT1/E1 network module that contains an NM-xDM network module may not allow incoming modem calls and generate the “no modem available” error message even though the output of the **show modem** command indicates that there is a free modem available.

  Conditions: This symptom is observed when frequent retrains occur on the modems.

  Workaround: There is no workaround.

- CSCed52163

  Symptom: When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as “OID not increasing” may occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured but HSRP is not configured at all.

Conditions: This symptom is observed under either one of the following two conditions:

- An SNMP HSRP query triggers a loop in the getnexts. Some MIB browsers catch this, and exit with a message stating “OID not increasing”.
- A scaling problem may occur with HSRP when there are a high number of tracked interfaces. For every standby track statement, every interface is tested to see if it is an HSRP tracked interface. No defined thresholds have been identified and tested that qualify when this scaling problem may occur. The more interfaces there are configured, the greater is the possibility that the problem occurs.

Workaround: Do not initiate an SNMP query for HSRP.

Alternate Workaround: Enter the **snmp-server** global configuration command to specify which MIBs are available, as in the following example:

snmp-server view *HSRP* **internet included**

snmp-server view *HSRP ciscoHsrpMIB* **excluded**

snmp-server view *HSRP ciscoHsrpExtMIB* **excluded**

snmp-server community public view *HSRP RW 20*

snmp-server community private view *HSRP RW 20*

- CSCed55962

  Symptoms: From a local customer edge (CE) router, you may not be able to reach or ping some prefixes (subnets) on a remote CE router over an Multiprotocol Label Switching (MPLS) network.

  Conditions: This symptom is observed in a cell-based MPLS network.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface that is connected to the local CE router. Doing so enables the Border Gateway Protocol (BGP) to run a scan again and repopulates the subnets in the Tag Forwarding Information Base (TFIB).

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In UserService (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCed83720

  Symptom: A router running SNASwitch enterprise extender over a WAN connection experiences intermittent performance problems.

  Conditions: This symptom is observed when some type of delay occurs in the IP network between the router and the third-party vendor host.

  Workaround: Take down the link. If this is not an option, there is no workaround.

  Further Problem Description: The Network Performance Monitor (NPM) on the mainframe reports network response times of up to 13 seconds and a display of the CNR node associated with the affected RTP pipe on the mainframe of the form "D NET,ID=CNR.....,E" shows that the allowed data flow rate is severely throttled.

  The problem usually lasts for about one hour before responses fall to acceptable subsecond levels but can take up to three hours to completely stabilize.

  No congestion, retransmissions are observed while the problem is occurring and a sniffer trace taken at the mainframe OSA port shows that the Round Trip Time (RTT) is consistently around 16 ms, which is acceptable, but the Server Measurement Interval (SMI), in the Rate Request coming from the mainframe, varies widely.

- CSCee20366

  Symptoms: IMA link status sticks in NE usable/usable while showing FE active/active.

  Conditions: This happens when connecting an IMA module in a Cisco 3640 to a third party vendor switch.

  Workaround: Administratively shut down the link and then bring it back.

- CSCee21038

  Symptoms: High CPU utilization occurs due to CEF scanner on a Cisco 7200 router that is running Cisco IOS Release 12.2(14)S7.

  Conditions: This symptom can happen when excessive number of layer 2 adjacency changes are happening, typically because of large number of continuous ARP messages. This could be because of a configuration issue or the router receiving such ARP messages from a peer on which there is no direct control.

  Workaround: There is no workaround.

- CSCee41492

  Symptoms: When a crypto map is applied to certain subinterface configurations, the IPSec SA path MTU is not always calculated correctly. This does not happen to every subinterface configuration and does not happen all the time. The root cause is related to the event handling when subinterface IP MTU is changed during the router initialization.

  Conditions: This symptom occurs when a crypto map is applied to certain subinterface configurations.

  Workaround: There is no workaround.

- CSCee41842

  Symptoms: "%TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag" error messages are seen in the log as MPLS labels are not being freed properly.

Conditions: This label leak problem has been noticed in BGP VPN when a locally learned VPN prefix becomes a remote prefix. This will happen if a set of routes has at least one local path via CE (could be EBGP learned or redistributed from VRF IGP) and one IBGP learned remote path. If the local CE learned path flaps for some reason, there is a possible label leak caused by BGP.

Workaround: Increase the label range using the **mpls label range x y** command.

- CSCee44279

  Symptoms: A Cisco router reboots more than once when using Cisco IOS Release 12.2(16b).

  Conditions: This problem is observed by doing the **shut** command followed by the **no shut** command on the ATM interfaces several times with traffic flowing through and by having QoS, service policy, and hardware encryption configured on ATM IMA interfaces.

  Workaround: Remove the service-policy prior to doing the **shut** command followed by the **no shut** command. Alternatively, stop the traffic prior to doing the **shut** command followed by the **no shut** command.

- CSCee49301

  Symptoms: On a Cisco 7500 series router with RSP based Multilink PPP enabled with FIFO queuing configured on multilink interfaces a very high number of lost received and lost fragments are seen on multilink interfaces. This problem is seen when MLPPP link is at 34-45%.

  Conditions: This symptom is observed on a Cisco 7500 series router with RSP based Multilink PPP enabled with FIFO queuing configured on the multilink interfaces. MLPPP link is at 34-45%.

  Workaround:

  1) Enable fair-queuing on multilink interfaces.

  2) Enable “transmit buffers backing-store” on the member links.

  3) It required to change the tx-queue-limit to 19 for T1 interfaces.

  4) Configure “multilink queuing bypass-fifo” which is a hidden command.

- CSCee49862

  Symptoms: A Cisco 7500 series multichannel T3 port adapter (PA-MC-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCee49983

  Symptoms: A Cisco 7500 Multichannel T3 Port Adaptor (PA-MC-2T3+) does not have a mechanism to report what type of alarm caused the controller to go down for short alarm duration conditions.

  This is an enhancement request to provide a history table of recent alarm conditions along with a corresponding timestamp to allow better troubleshooting information to be gathered.

  Workaround: There is no workaround.

- CSCee58562

  Symptoms: A Cisco router may reload under a specific sequence of CLI commands:

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#policy-map Set_BestEffort_IP
(config-pmap)#class class-default
(config-pmap-c)#shape average 4000000
shape is invalid command in input policy.
```

```
(config-pmap-c)#exit
(config-pmap)#exit
(config)#interface Serial4/1/0:10
(config-if)#bandw 4096
...router reloads...
```

Conditions: This symptom has been observed in Cisco IOS Release 12.2(13)T and Release 12.3(6) software, but it should be reproducible in older Cisco IOS releases as well.

Workaround: Avoid the illegal **shape** command.

- CSCee58796

  Symptom: The router is unable to poll dsx1ConfigTable for WIC-CSUDSU module.

  Condition: This problem is observed when a Cisco 3600 router has WIC-CSUDSU-T1 module and is running Cisco IOS Release 12.2(23a).

  Workaround: There is no workaround.

- CSCee61646

  Symptoms: The problem exists when PIM announcement packets are distributed through tunnels, and when crypto map, which specifies the protection on GRE traffic, is only applied to the physical interface. Even though it is a correct way to apply the crypto map only to the physical interface to protect the GRE traffic, the crypto policy checking on PIM announcement packets is missing.

  Conditions: This symptom occurs when PIM announcement packets are distributed through tunnels.

  Workaround: Apply the crypto map to both tunnel and physical interfaces.

- CSCee74111

  Symptoms: A Cisco voice gateway may reload with a bus error at an invalid address and generate the following error message:

  System was restarted by bus error at by bus error at PC 0x60C7D834, address 0xD0D0D23

  Conditions: This symptom is observed on a Cisco voice gateway that runs Cisco IOS Release 12.2(23b) and that is configured for H.323. The symptom may also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCee82681

  Symptoms: RSP does not report input or output packets on an RTR probe.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(23a) or Release 12.3 and is more likely to occur when the number of channelized port adapters such as the PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters that are installed in the router is high.

  Workaround: Reload the router.

  Alternate Workaround: Reload microcode on the port adapter that are installed in the router.

- CSCin68712

  Symptoms: A Cisco 7500 series router may reload when multilink interface configured on the router comes up.

  Conditions: This symptom would happen if service-policy is configured on the multilink interface and distributed switching is enabled.

  Workaround: Not configuring service-policy on the router would prevent the router from reloading.

- CSCuk50878

  Symptoms: After a number of WCCP “cache lost” and “cache found” events have occurred on a Cisco router, spurious memory accesses may occur, and then the addition and deletion of WCCP services may fail. When this situation occurs, the output of the **show ip wccp** *service-number* command does not show the WCCP service, even though the WCCP service does show in the output of the **show ip wccp** command.

  Conditions: This symptom is observed only on Cisco IOS images that contain the fix for CSCec55429 and only with dynamic services (not with web cache service) when all the caches in a service group are lost and then reacquired a number of times. Such a situation may occur by services being manually disabled and reenabled on a cache or by a heavy traffic load between the router and the cache, causing WCCP protocol messages to be dropped.

  Once the symptom has occurred, you must stop all WCCP services on the router, and then restart the WCCP services.

  Workaround: There is no workaround.

- CSCuk51269

  Symptoms: Multicast packets such as HSRP and OSPF are not received on a port-channel interface.

  Conditions: This symptom is observed when a port-channel interface is configured on a Cisco router, when you reload the router, and when the first member is added to the port-channel interface by entering the **no shutdown** interface configuration command on physical interface.

  Workaround: Enter the do **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port-channel interface.

- CSCuk51673

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled and the following error message may appear on the console:

  %FIB-3-NOMEM: Malloc Failure, disabling DCEF

  %FIB-2-FIBDOWN: CEF has been disabled due to a low memory condition.

  It can be re-enabled by configuring “ip cef [distributed]”

  Conditions: This may be seen on a platform running DCEF.

  Workaround: Upgrade to the image containing this bug-fix.

Resolved Caveats—Cisco IOS Release 12.2(24b)

Cisco IOS Release 12.2(24b) is a rebuild release for Cisco IOS Release 12.2(24). The caveats in this section are resolved in Cisco IOS Release 12.2(24b) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCed52163

  Symptom: When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as “OID not increasing” may occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured.

  Conditions: This symptom is observed under either one of the following two conditions:

  - An SNMP HSRP query triggers a loop in the getnexts. Some MIB browsers catch this, and exit with a message stating “OID not increasing”.

  - A scaling problem may occur with HSRP when there are a high number of tracked interfaces. For every standby track statement, every interface is tested to see if it is an HSRP tracked interface. No defined thresholds have been identified and tested that qualify when this scaling problem may occur. The more interfaces there are configured, the greater is the possibility that the problem occurs.

  Workaround: Do not initiate an SNMP query for HSRP.

  Alternate Workaround: Enter the **snmp-server** global configuration command to specify which MIBs are available, as in the following example:

  snmp-server view *HSRP* **internet included**

  snmp-server view *HSRP ciscoHsrpMIB* **excluded**

  snmp-server view *HSRP ciscoHsrpExtMIB* **excluded**

  snmp-server community public view *HSRP RW 20*

  snmp-server community private view *HSRP RW 20*

- CSCed55962

  Symptoms: From a local customer edge (CE) router, you may not be able to reach or ping some prefixes (subnets) on a remote CE router over an Multiprotocol Label Switching (MPLS) network.

  Conditions: This symptom is observed in a cell-based MPLS network.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface that is connected to the local CE router. Doing so enables the Border Gateway Protocol (BGP) to run a scan again and repopulates the subnets in the Tag Forwarding Information Base (TFIB).

- CSCed83720

  Symptom: A router running SNASwitch enterprise extender over a WAN connection experiences intermittent performance problems.

  Conditions: This symptom is observed when some type of delay occurs in the IP network between the router and the third-party vendor host.

  Workaround: Take down the link. If this is not an option, there is no workaround.

Further Problem Description: The Network Performance Monitor (NPM) on the mainframe reports network response times of up to 13 seconds and a display of the CNR node associated with the affected RTP pipe on the mainframe of the form “D NET,ID=CNR.....,E” shows that the allowed data flow rate is severely throttled.

The problem usually lasts for about one hour before responses fall to acceptable subsecond levels but can take up to three hours to completely stabilize.

No congestion, retransmissions are observed while the problem is occurring and a sniffer trace taken at the mainframe OSA port shows that the Round Trip Time (RTT) is consistently around 16 ms, which is acceptable, but the Server Measurement Interval (SMI), in the Rate Request coming from the mainframe, varies widely.

- CSCee21038

  Symptoms: High CPU utilization occurs due to CEF scanner on a Cisco 7200 router that is running Cisco IOS Release 12.2(14)S7.

  Conditions: This symptom can happen when excessive number of layer 2 adjacency changes are happening, typically because of large number of continuous ARP messages. This could be because of a configuration issue or the router receiving such ARP messages from a peer on which there is no direct control.

  Workaround: There is no workaround.

- CSCee41492

  Symptoms: When a crypto map is applied to certain subinterface configurations, the IPSec SA path MTU is not always calculated correctly. This does not happen to every subinterface configuration and does not happen all the time. The root cause is related to the event handling when subinterface IP MTU is changed during the router initialization.

  Conditions: This symptom occurs when a crypto map is applied to certain subinterface configurations.

  Workaround: There is no workaround.

- CSCee41842

  Symptoms: “%TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag” error messages are seen in the log as MPLS labels are not being freed properly.

  Conditions: This label leak problem has been noticed in BGP VPN when a locally learned VPN prefix becomes a remote prefix. This will happen if a set of routes has at least one local path via CE (could be EBGP learned or redistributed from VRF IGP) and one IBGP learned remote path. If the local CE learned path flaps for some reason, there is a possible label leak caused by BGP.

  Workaround: Increase the label range using the **mpls label range x y** command.

- CSCee49301

  Symptoms: On a Cisco 7500 series router with RSP based Multilink PPP enabled with FIFO queuing configured on multilink interfaces a very high number of lost received and lost fragments are seen on multilink interfaces. This problem is seen when MLPPP link is at 34-45%.

  Conditions: This symptom is observed on a Cisco 7500 series router with RSP based Multilink PPP enabled with FIFO queuing configured on the multilink interfaces. MLPPP link is at 34-45%.

  Workaround:

  1) Enable fair-queuing on multilink interfaces.

  2) Enable “transmit buffers backing-store” on the member links.

  3) Change the tx-queue-limit to 19 for T1 interfaces is required.

- CSCee49862

  Symptoms: A Cisco 7500 series multichannel T3 port adapter (PA-MC-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCee61646

  Symptoms: A multicast packet is not correctly encrypted through IPSec and GRE.

  Conditions: This symptom is observed when PIM announcement packets are distributed through tunnels and when the crypto map that specifies the protection on the GRE traffic is only applied to the physical interface. Even though this is a correct way to apply the crypto map only to the physical interface to protect the GRE traffic, crypto policy checking is missing on PIM announcement packets.

  Workaround: Apply the crypto map to both the tunnel interface and the physical interface.

- CSCin75294

  Symptoms: The **show controller T3** command does not show T1 level alarm history. Alarm history is not maintained at T1 level.

  Conditions: This symptom is observed on Cisco 7500 series routers.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCec66723

  Symptoms: Cisco IOS TCP backs off for second packet in retransmission Queue.

  Conditions: When the TCP stack has couple packets in the retransmission queue, it means that these packets were either dropped in the network or were not reliably received by the remote end. Under this condition, TCP goes into slow start, sends the first packet in the retransmission queue and backs off the retransmission timer. This repeated till we get an ACK for the packet. No other packet in the retransmission queue is sent unless we get the ACK for the earlier packet in the retransmission queue. When the ACK comes in, TCP is supposed to retain the same krtt values for sending the next packet in the queue. However, IOS TCP backs off yet again, causing a slightly slower sending of packets in the retransmission queue. The impact of this is supposed to be minimal. Once the packets in the retransmit queue are cleared (ACKed), TCP will return to its old state of sending data up to the window advertised by the peer.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(24a)

All of the Catalyst 5000 RSM/VIP2 images have been deferred in Cisco IOS Release 12.2(24a). The software solution is Cisco IOS Release 12.2(24b). See the caveats listed under “Resolved Caveats—Cisco IOS Release 12.2(24b).”

Resolved Caveats—Cisco IOS Release 12.2(24)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(24). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(24). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCdz32659

  Symptoms: Many memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  Conditions: The symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(17)ST. The symptom may also occur on other Cisco 7500 series routers that run Release 12.0 S, 12.2 S, 12.3, or 12.3 T.

  Workaround: To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCea33897

  Symptoms: A Cisco router may generate a "%SYS-2-LINKED: Bad requeue" message. Following this message and after a time of operation, memory fragmentation occurs and the router reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(11)T. However, the symptom is not platform specific nor release specific.

  Workaround: There is no workaround.

- CSCed09685

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

- CSCed33110

  Symptoms: A VIP crash can lead to a memory exhaustion situation on the RSP in turn leading to an RSP crash.

  Conditions: This will happen more frequently on routers with a high idb count.

  Workaround: There is no workaround.

- CSCed44414

  Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

  Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

  Workaround: There is no workaround.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

IBM Connectivity

- CSCeb65576

  Symptoms: A Cisco 2620 may reload because of a segmentation violation (SegV).

  Conditions: This symptom is observed when you attempt to run X.25 (at packet level) over a Logical Link Control, type 2 (LLC2) (at frame level) from a third-party vendor workstation to the Cisco 2620.

  This problem was also seen when running DLSw (Data Link Switching).

  Workaround: There is no workaround.

- CSCed77737

  Symptoms: Data-link switching (DLSw) Synchronous Data Link Control (SDLC) does not send an XID command. The DLSw circuit does go into the CONNECTED state, but it stays in the CKT_ESTABLISHED state until it drops.

  Conditions: This symptom is observed when SDLC attaches to a PU2.0 and attempts to establish a session via DLSw to an Ethernet-attached Tandem where the DLSw SDLC interface is running as a role primary. After the DLSw router sends an XID P and the Tandem returns an XID F, the DLSw router does not send an XID command.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCdv57198

  Symptoms: A Cisco router may forward the MAC-layer broadcast.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1(10) but may also occur in other releases.

  Workaround: There is no workaround.

- CSCin40163

  Symptoms: An ATM interface may remain administratively down.

  Conditions: This symptom is observed when commands do not have any effect because the command-line interface (CLI) does not function. The symptoms are platform independent.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeb40561

  Symptoms: A Cisco router may reload if it is low on processor memory and Simple Network Management Protocol (SNMP) get operations are performed on Open Shortest Path First (OSPF) MIBs.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(8)YW, Release 12.2(8)YY, Release 12.2 T, Release 12.3, or Release 12.3 T.

  Workaround: There is no workaround.

- CSCed81271

  Symptoms: If using IGMP static join groups with the Cisco 2600 FastEthernet modules, it may be that the groups do not get re-added if the cable is disconnected and then reconnected to the interface.

  Conditions: This symptom is observed on a Cisco 2600 series but may also occur on other platforms.

  Workaround: Use the **clear ip mroute *** command in privileged EXEC mode.

- CSCed90268

  Symptoms: NAT calculates an invalid UDP checksum for some checksum values.

  Conditions: This symptom is observed in a very particular situation which depends on the NAT configuration and the UDP checksum value. After the translation, the new UDP checksum value of the translated packet is equal to zero. NAT ignores the new checksum value of zero, and it uses the original checksum value, which causes a checksum error at the end device.

  Workaround: There is no workaround.

Miscellaneous

- CSCea15783

  Symptoms: A Cisco 3640 router that is configured with a Systems Network Architecture Switch (SNASwitch) reloads unexpectedly and displays the following message:

  System was restarted by bus error

  Conditions: This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(15).

  Workaround: There is no workaround.

- CSCea24089

  Symptoms: The serial communication controller in an asymmetric digital subscriber line (ADSL)-ATM interface that is installed in an NM-FE2W or NM-2W network module may lock up in the receiving path and does not recover.

Conditions: This symptom is observed when the ADSL-ATM interface is stressed to 10 Mbps downstream.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCea62212

  Symptoms: While reading or writing from/to an ATA flash device, you may see an ATA_status timeout error. While formatting an ATA flash device, you may see an unknown error.

  Conditions: This symptom is observed on any Cisco IOS image containing the fix for CSCdw51692.

  Workaround: There is no workaround.

- CSCeb60421

  Symptoms: A Cisco AS5300 may reload unexpectedly. The output of the **show version** command may show an error message similar to the following:

  System restarted by software forced crash at 0x6037EE44

  Conditions: This symptom is observed on a Cisco AS5300 that runs Cisco IOS Release 12.2(19). The symptom could also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCeb69570

  Symptoms: You may not be able to start a new session on a Cisco router that runs Systems Network Architecture switching services (SNASw). The log may indicate sense code 08150004 (“LSFID already in use”); the log of the host may indicate sense code 08390001.

  Conditions: This symptom is observed when a user logs off and then attempts to log back on at a later time.

  Workaround: Reload the router.

- CSCec03907

  Symptoms: A Route Switch Processor 4 Plus (RSP4+) may reload.

  Conditions: This symptom is observed on a Cisco 7500 series when you configure the **interface loopback** *interface-number* interface configuration command on an interface of the router and the value of the *interface-number* argument is a 9-digit number that starts with 10.

  Workaround: If possible, use another range of numbers for the numbers that are assigned to the loopback interfaces, that is, a range of numbers that do not start with 10.

- CSCec33028

  Symptoms: A 1-port E3 serial port adapter (PA-E3) may fail to recover to the “up/up” state even when the original cause of the failure is corrected.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the PA-E3.

- CSCec76965

  Symptoms: When configuring QoS on a Cisco 7200 series, the router may reload with a bus error. Specifically, the bus error occurs after having entered the **no class** *name* command on subinterfaces.

  Conditions: This symptom is observed on a Cisco 7200 series that runs the c7200-jk9s-mz image of Cisco IOS Release 12.2(17a). The symptom may also occur in other releases. This behavior is associated to the use of “payload-compression.”

Workaround: There is no workaround.

- CSCec80784

  Symptoms: A memory leak may occur in the "ATMSIG Input" process.

  Condition: This symptom is observed on a Cisco 7500 series Route Switch Processor (RSP) that runs Cisco IOS Release 12.2(16a) or Release 12.2(19a) when ATM Address Resolution Protocol (ARP) is configured and when switched virtual circuit (SVC) collisions occur while ARP map lists are being populated. The symptom may also occur in Release 12.3 or Release 12.3 T.

  Workaround: There is no workaround.

- CSCec83427

  Symptoms: A router may reload when forwarding voice calls received on a BRI interface.

  Conditions: This symptom occurs when the router is configured as a voice gateway.

  Workaround: There is no workaround.

- CSCec86420

  Symptoms: When you enter the **undebug all** privileged EXEC command on a Cisco 3700 series, all traffic that passes through an encrypted generic routing encapsulation (GRE) tunnel may stop.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured with a GRE tunnel that is secured via IP Security (IPSec) and that is using Cisco Express Forwarding (CEF) switching.

  Workaround: Reinitialize CEF switching by entering the **no ip cef** global configuration command followed by the **ip cef** global configuration command.

  Alternate Workaround: Do not enter the **undebug all** privileged EXEC command. Rather, individually disable each **debug** command.

- CSCed19669

  Symptoms: Some calls experience one way voice where the caller hears nothing. The problem worsens as more time passes.

  Conditions: This problem occurs in a Cisco AS5800 that is running c5800-p4- mz.122-7d.bin and works as VoIP ingress gateway.

  Workaround: Reload DSP module.

- CSCed21717

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCed30670

  Symptoms: An H.323 proxy may fail when a conference call between a PSTN user and IP phones users is initiated by an IP phone in a Cisco CallManager environment.

Conditions: This symptom is observed on a Cisco router that functions as a gatekeeper, that has the H.323 proxy enabled, and that runs Cisco IOS Release 12.3(5) in the following topology:

An IP phone connects to a Cisco CallManager that connects to the Cisco gatekeeper that has the H.323 proxy enabled. The Cisco gatekeeper connects to yet another gatekeeper that connects to a gateway that, in turn, connects to the PSTN.

All calls to and from the Cisco CallManager IP phone via the Cisco gatekeeper are proxied. The Cisco CallManager runs software version 3.3(3)SR3. The display IE delivery option is disabled in the H.225 trunk configuration in the Cisco CallManager administration web page. The H.225 trunk is controlled by one of the gatekeepers.

The symptom occurs in the following sequence of events:

1. A PSTN user calls IP phone (IP phone 1).

2. The user of IP phone 1 answers the call and the call is connected with two-way audio.

3. The user of IP phone 1 presses the “conference” button and calls another IP phone (IP phone 2).

4. The user of IP phone 2 answers the call and the call is connected with two-way audio.

5. The user of IP phone 1 presses the “conference” button again.

6. The H.323 proxy fails, causing the PSTN to be disconnected from the conference call.

7. The conference call continues between the user of IP phone 1 and the user of IP phone 2.

Workaround: Enable the “Display IE delivery” option in the H.225 trunk configuration Cisco CallManager administration web page.

Alternate Workaround: Disable the H.323 proxy on the Cisco gatekeeper.

- CSCed35253

  Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

  Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

  Workaround: Disable IP Inspect and IDS.

- CSCed39059

  Symptoms: The tag forwarding table for a line card on Cisco platforms that have distributed (i.e. line card based) forwarding, such as the Cisco 7500 Series and the Cisco 12000 Series, may not have complete entries even though the Route Processor (RP) does. This results in ingress tagged traffic being dropped for the missing tag forwarding entries.

  Conditions: This symptom is observed on Cisco platforms that have distributed (i.e. line card based) forwarding in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment with a provider edge (PE) router to customer edge (CE) router link.

  The problem is more likely to happen if the PE to CE link experiences quick flaps of an interface (i.e. goes down and come back up in a very small amount of time (e.g. 2 sec)). Although this can happen on any line card, this situation is more likely to happen on the Engine 3(E3) channelized OC48 line cards due to its quick flapping behavior.

  Note: There are additional prerequisites for this bug to happen. These are:

  - The defect affects routers that are: (a) MPLS VPN PE routers or (b) routers that exchange labels for ipv4 BGP routes.

  - For (a) there should be recursive routes on the PE that go over the PE-CE link (this could be either BGP learnt recursive routes or static recursive routes). Also, these recursive routes have the link’s CE side IP address as their nexthop.

- There should be a less specific route to get to the nexthop (this can be a default route). This applies for (a) and (b).

Workaround: There is no workaround.

- CSCed41231

  Symptoms: An alignment error may cause a Cisco router to reload unexpectedly.

  Conditions: This symptom is observed under rare conditions (an “extreme corner case”) on a MIPS-based Cisco platform or on a Versatile Interface Processor (VIP), port adapter, or line card that contains a MIPS processor. The symptom is not release-dependent and may occur in all Cisco IOS releases.

  Workaround: There is no workaround.

  Further Problem Description: All 7500 VIPs and 7200 NPEs use MIPS based processors. Additional platforms that use MIPS processors:

  2691,3620,3631,3640,3660,3725,3745,4500,4500-M,4700,4700-M,AS5300,AS5400,AS5450, AS5800 Router Shelf,AS5800 System Controller (3640 based),7120,7140,UBR7100, UBR7200 - All NPE’s,7301,7304,7400,6500 MSFC,6500 MSFC2,7600 MSFC,7600 MSFC2, 10000,UBR10012,12000 GRP, most (if not all) 12000 Line Cards

- CSCed44319

  Symptoms: A file that is copied to an ATA disk may become corrupted.

  Conditions: This symptom is observed on any Cisco IOS image that contains the fix for CSCdz27200. The problem does not occur on a disk that is formatted with 16 or less sectors/cluster.

  Workaround: Use an ATA disk that is formatted with 16 or less sectors/cluster.

- CSCed45746

  Symptoms: Several prefixes for non-redistributed connected interfaces in different VRFs may be partially bound to the same MPLS-VPN label, thus disrupting traffic bound to one or more of these VRFs.

  Conditions: This symptom can occur on a Cisco router that runs Cisco IOS Releases 12.2, 12.2T, 12.0S, 12.3 after the VRF interfaces have flapped. The symptom may occur in all code levels of these releases.

  Workaround: Clear the routes in the VRFs in sequence.

- CSCed46937

  Symptoms: Sessions may fail with sense code 08150004.

  Conditions: This symptom is observed when an SNA switching services Enterprise Extender (EE) is used to connect to a host. New sessions that attempt to reuse an existing EE RTP connection to the host may fail with sense code 08150004. Other RTP connections do accept new sessions.

  Workaround: Inactivate the flawed RTP connection on the host. Doing so drops all existing sessions on that RTP connection, but enables the router and all other RTP connections and their sessions to stay up.

- CSCed47409

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), a router may reload after accessing a freed Label Information Base (LIB) entry. When the symptom occurs, an error message similar to the following is likely to precede the reload:

  ```
  %TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13
  ```

Conditions: This symptom is observed when a very uncommon timing of a Label Distribution Protocol (LDP) events occurs. The symptom may occur with LDP or Tagswitching Distribution Protocol (TDP).

Workaround: There is no workaround.

- CSCed50932

  Symptoms: The following error message is generated in a SNASw router while bringing up CP-CP sessions with a network node server:

  ```
  %SNASW-3-DS_LOG_17: PROBLEM - 22702 - Protocol error while registering resources with
  network node server
  ```

  Sense code 1014023C is returned by the NN server on the registration failure notification. The SNASw router unbinds the CP-CP sessions with sense code 08900060.

  Conditions: This symptom is observed on a Cisco router that functions as an SNASw router when a downstream end node incorrectly registers an APPN network node as an end node.

  Workaround: Remove the CP name on the partner LU definition on the downstream end node.

  Alternate Workaround: Apply APAR JR16282 to the downstream end node.

- CSCed51523

  Symptoms: The **show** *flash-filesystem* EXEC command and the **dir** *filesystem* EXEC command may not work properly on a Cisco 2600XM, preventing you from seeing the flash images.

  In addition, the **copy** *destination url* **flash:** EXEC command may fail when the **erase** option is not selected (that is, you type in **no** when you are asked if you want to erase the device). The **copy** *destination url* **flash:** EXEC command functions fine when you do select the **erase** option.

  Conditions: These symptoms are observed on a Cisco 2600XM that is configured with a particular third-party vendor 16-MB SIMM. Note that the router is still functional with this SIMM; you can boot or reload the router, perform a TFTP download operation, and similar actions without any difficulty.

  Workaround: There is no workaround.

- CSCed57204

  Symptoms: When a large number of VRFs are configured, input OAM F5 loopback cells on the ATM interface are dropped continuously even without traffic. Drop could be seen at OAM cell drops of **show atm traffic** and at Input queue drops of **show interface ATM** EXEC commands.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(19), Release 12.3(5), or Release 12.3(4)T2 where the **oam-pvc manage** command and the **ip vrf** global command are configured.

  Workaround: Remove the **ip vrf** command. Workaround is none for the router that could not remove VRFs such as Provider Edge (PE) router.

- CSCed57482

  Symptoms: A Cisco router may reload unexpectedly with a bus error when under stress.

  Conditions: Dynamic crypto map is being used in this IPSec responder router with Cisco IOS Release 12.2(any). Router is under stress and/or number of established IPSec tunnels reached the HW engine's flow limit.

  This crash is not seen with Cisco IOS Releases 12.2 T, 12.3, or 12.3 T but only with Release 12.2.

  Workaround: Use static crypto maps instead of dynamic crypto maps. Lower the stress level and/or number of IPSec tunnels.

- CSCed83744

  Symptoms: One way audio issues are observed in a network.

  Conditions: This symptom is observed on a Cisco AS5800 series universal gateway.

  Workaround: There is no workaround.

- CSCed88967

  Symptoms: When you enter the **write memory** command, two files may be missing ("persistent-data" and "rf_cold_starts") or the following error message may be displayed:

  ```
  startup-config file open failed (Device or resource busy)
  ```

  Conditions: This symptom is observed on any router with redundant RPs running any Cisco IOS release when the following sequence occurs:

  - You enter the **write memory** command on the console of the master RP.

  - The NVRAM of the standby RP is accessed by a local application (that is, the application on the standby RP).

  - A switchover occurs.

  Workaround: Do not access the NVRAM of the standby RP when you enter **write memory** command on the console of the master RP.

- CSCee06794

  Symptoms: DTS may not work properly on dot1q Fast Ethernet subinterfaces. Traffic is not shaped at the expected rate

  Conditions: This problem is observed on a Cisco 7500 series router that is configured as a PE router and that runs Cisco IOS Release 12.2(12i). The symptom may also occur in other releases.

  Workaround: If this is an option, use ISL subinterfaces.

- CSCee10916

  Symptoms: A Cisco 3640 series router may encounter software forced crashes due to memory corruptions.

  Conditions: This symptom is observed on a Cisco 3640 series router that is running Cisco IOS Release 12.2(21a).

  Workaround: The following are possible workarounds:

  - downgrade to Cisco IOS Release 12.2(17), or

  - disable snmp (or possibly just disable "snmp-server enable traps voice poor- qov").

- CSCin56408

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCin57765

  Symptoms: A router may become unresponsive and may reload when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) flash card (for example, boot disk, disk0, disk1).

  For example, this situation may occur when you enter the **show** *command* **| tee /append** *url* privileged EXEC command.

  Conditions: This symptom is observed on a Cisco platform that runs a Cisco IOS image that contains the fix for caveat CSCdz27200 and that utilizes an ATA flash card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz27200. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Write the output of the **show** command to a new file instead of appending it to an existing file by entering the **show** *command* **| tee** *url* privileged EXEC command.

- CSCin65147

  Symptoms: A VC that is configured on an IMA interface may remain in the inactive state.

  Conditions: This symptom is observed when the VC is in the inactive state while the links come up. In this situation, the VC should enter the "up" state, but does not do so.

  Workaround: Remove and reconfigure the VC.

- CSCin66542

  Symptoms: The line protocol on a T1 of a T3 controller in a PA-MC-2T3+ port adapter may stay in the down state even when looped.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

- CSCin68517

  Symptoms: A Cisco router that is running Cisco Gateway GPRS Support Node (GGSN) software may show high CPU usage if deletion of a lot of PDP contexts is initiated from the GGSN side.

  Conditions: Such deletion of a lot of PDPs from GGSN can be initiated from GGSN when the **clear** command is issued for all PDPs or all PDPs of a path/apn etc., or, if the update request is received on a path with a different restart count at a point when the path has lot of PDP contexts belonging to it.

  Workaround: There is no workaround.

- CSCuk44928

  Symptoms: When you save a configuration first to the standby Performance Routing Engine (PRE) and then to the active PRE, the configuration may not be saved and the following error message may be generated:

  startup-config file open failed (Device or resource busy)

  Conditions: This symptom is observed on a Cisco 10000 series and c7500, that is configured with redundant PREs and that runs Cisco IOS Release 12.0(26)S. The symptom may also occur in other Cisco IOS releases.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCdz35342

  Symptoms: A router may reload because of a watchdog timeout if the **no dialer pool-member** interface configuration command is entered on the D channel of the router.

  Conditions: This symptom is observed on a Cisco router when the command is entered on the D channel and there is more than one link that is bound to the dialer profile with Multilink PPP (MLP).

  Workaround: Shut down the dialer interfaces and physical interfaces that are relevant to the dialer pool. After the interfaces are completely down, enter the **no dialer pool-member** interface configuration command.

- CSCec83030

  Symptoms: A parity error on a Versatile Interface Processor (VIP) card may cause other VIPs to go to a wedged state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCed21813

  Symptoms: A Cisco 7204VXR in which an enhanced 1-port ATM OC-3c/STM-1 port adapter (PA-A3-OC3) is installed may reload unexpectedly because of a bus error. However, the cause of the symptom may be a segmentation and reassembly (SAR) chip failure that occurs because of an "Address Error (store) exception."

  Conditions: This symptom is observed on a Cisco 7204VXR that is configured for Dynamic Bandwidth Selection (DBS) support when you attempt to modify the VC QoS parameters under high traffic conditions.

  Workaround: Shut down the ATM interface before attempting to modify the VC QoS parameters.

- CSCed40110

  Symptoms: When a router running Cisco IOS Release 12.0S, 12.1, 12.2, or 12.2T receives a multilink packet with Protocol Field Compression (PFC) applied, the packet is not interpreted correctly, and is subsequently rejected. The following debug messages appear in the debug trace when the **debug ppp negotiation** command is enabled:

  ```
  MLP: I UNKNOWN(192) [Not negotiated] id 0 len 0 LCP: O PROTREJ [Open] id 2 len 95
  protocol MLP
  ```

  Conditions: This symptom is observed when the router requests PFC during Link Control Protocol (LCP) negotiations and the peer applies PFC to its outbound packets. PFC is enabled by default on asynchronous serial interfaces, it is disabled by default on other interfaces.

  Workaround: In Cisco IOS Release 12.2 and 12.2T, PFC can be disabled using the **ppp pfc local forbid** interface configuration command. In Release 12.0S and 12.1, there is no workaround.

- CSCed69664

  Symptoms: Every 128th call on a BRI/PRI interface may have the wrong CallRef.

  Conditions: This symptom is observed when you make ISDN calls on a Cisco platform that has a BRI/PRI interface. The CallRef increases from 0x01 to 0x7F for BRI/PRI calls. After 0x7F, if the 128th call is on a BRI and the switch type to which the platform is connected only supports a 1-byte CallRef, the call fails.

  Workaround: There is no workaround. However, only every 128th call fails. Calls after the 128th call work fine.

- CSCed73619

  Symptoms: An ATM ABR SVC setup could fail while an UBR SVC can succeed.

  Conditions: This symptom is observed when an illegal ICR value occurs.

  Workaround: There is no workaround.

- CSCed78461

  Symptoms: While the traffic is flowing, if async configuration is removed or async link flaps, causing the PPP session to be broken, then the router may crash.

  Conditions: This symptom is observed under the following conditions:

  1. Traffic still needs to be running

  2. Async configuration while the network is intact

  3. PPP encapsulation

  Workaround: There is no workaround.

  Further Problem Description: This is not a very high impact as the timing window for this problem to happen is very small.

- CSCin50541

  Symptoms: A router may reload after you enter the **ppp multilink** interface configuration command.

  Conditions: This symptom occurs when multilink is configured on an active serial interface and neither the **ppp multilink group** interface configuration command nor the **multilink virtual-template** global configuration command is entered. Under these conditions, multilink normally fails to create a bundle because of the lack of a configuration source for the bundle interface, but in this instance, it causes the router to reload.

  Workaround: Enter the **shutdown** interface configuration command to shut down the serial interface. Then, enter the **ppp multilink group** interface configuration command on the serial interface.

Resolved Caveats—Cisco IOS Release 12.2(23f)

Cisco IOS Release 12.2(23f) is a rebuild release for Cisco IOS Release 12.2(23). The caveats in this section are resolved in Cisco IOS Release 12.2(23f) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

Miscellaneous

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Resolved Caveats—Cisco IOS Release 12.2(23e)

Cisco IOS Release 12.2(23e) is a rebuild release for Cisco IOS Release 12.2(23). The caveats in this section are resolved in Cisco IOS Release 12.2(23e) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Miscellaneous

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

- CSCef44225

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Resolved Caveats—Cisco IOS Release 12.2(23d)

Cisco IOS Release 12.2(23d) is a rebuild release for Cisco IOS Release 12.2(23). The caveats in this section are resolved in Cisco IOS Release 12.2(23d) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCee22810

  Symptoms: A Cisco 7500 may experience a random status down of all PVCs at once for about 2 minutes before they come back up. During the DLCI down status, the subinterface does not go down and no notifications were observed in the message log.

  Conditions: This has been observed on multiple Cisco 7500 routers with RSP8 or RPS4+ running version rsp-jsv-mz.122-12i with Frame Relay configured on an 8-port port adapter and HSSI for 450+PVC/DLCIs.

  Workaround: There is no workaround.

- CSCee74111

  Symptoms: A Cisco voice gateway may reload with a bus error at an invalid address and generate the following error message:

  System was restarted by bus error at by bus error at PC 0x60C7D834, address 0xD0D0D23

  Conditions: This symptom is observed on a Cisco voice gateway that runs Cisco IOS Release 12.2(23b) and that is configured for H.323. The symptom may also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCee80885

  Symptoms: A Cisco voice gateway may reload with a bus error at an invalid address:

  System was restarted by bus error at PC 0x60C5BD30, address 0xD391832C

  Conditions: This symptom is observed on a Cisco voice gateway that is running Cisco IOS Release 12.2(23b) and H.323.

  Workaround: There is no workaround.

- CSCef03016

  Symptoms: The line protocol on a PA-E3 serial interface may go down at random. During this time the **show interface serial x/y** command will show that the output queue is wedged (Output queue: 40/40) and that output drops are increasing.

  Conditions: This symptom occurs when a Cisco 7204VXR router is equipped with a PA-E3 module and is configured for the following:

  -**encapsulation frame-relay**, **frame-relay traffic-shaping** and **tx-ring-limit x** on the PA-E3 serial interface -multiple point-to-point subinterfaces with different Frame Relay Traffic Shaping (FRTS) parameters applied on each of the interfaces, and Class Based Weighted Fair Queueing (CBWFQ) applied on some of the interfaces

  Workaround: Either configure **shutdown** followed by **no shutdown** on the PA-E3 serial interface, or enter **clear interface serial x/y**.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Resolved Caveats—Cisco IOS Release 12.2(23c)

Cisco IOS Release 12.2(23c) is a rebuild release for Cisco IOS Release 12.2(23). The caveats in this section are resolved in Cisco IOS Release 12.2(23c) but may be open in previous Cisco IOS releases.

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.

Interfaces and Bridging

- CSCeb81473

  Symptoms: A Cisco 7500 series that is configured as a bridge may not pass bridged traffic on a FDDI interface. This situation may lead to a loss of connectivity.

  Conditions: This symptom is observed on Cisco 7500 series that runs a Cisco IOS rsp-jsv-mz image.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the FDDI interface.

Miscellaneous

- CSCee41842

  Symptoms: “%TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag” error messages are seen in the log as MPLS labels are not being freed properly.

  Conditions: This label leak problem has been noticed in BGP VPN when a locally learned VPN prefix becomes a remote prefix. This will happen if a set of routes has at least one local path via CE (could be EBGP learned or redistributed from VRF IGP) and one IBGP learned remote path. If the local CE learned path flaps for some reason, there is a possible label leak caused by BGP.

  Workaround: Increase the label range using the **mpls label range x y** command.

Resolved Caveats—Cisco IOS Release 12.2(23a)

Cisco IOS Release 12.2(23a) is a rebuild release for Cisco IOS Release 12.2(23). The caveats in this section are resolved in Cisco IOS Release 12.2(23a) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCdz32659

  Symptoms: Many memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of
  -1732547824 bytes failed from x605111F0, pool Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  Conditions: The symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(17)ST. The symptom may also occur on other Cisco 7500 series routers that run Release 12.0 S, 12.2 S, 12.3, or 12.3 T.

  Workaround: To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCed09685

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

- CSCed33110

  Symptoms: A VIP crash can lead to a memory exhaustion situation on the RSP in turn leading to an RSP crash.

  Conditions: This will happen more frequently on routers with a high idb count.

  Workaround: There is no workaround.

- CSCed44414

  Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

  Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

  Workaround: There is no workaround.

- CSCin67568

  Symptoms: A Cisco Catalyst 2950 experiences a memory leak in the CDP process.

  Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

IP Routing Protocols

- CSCed81271

  Symptoms: If using IGMP static join groups with the Cisco 2600 FastEthernet modules, it may be that the groups do not get re-added if the cable is disconnected and then reconnected to the interface.

  Conditions: This symptom is observed on a Cisco 2600 series but may also occur on other platforms.

  Workaround: Use the **clear ip mroute *** command in privileged EXEC mode.

Miscellaneous

- CSCdy40928

  Symptoms: Connectivity difficulties may occur when Virtual Private Network (VPN) routing/forwarding (VRF) packets follow the global routing table instead of the VRF table.

  Conditions: This symptom is observed on a low-end Cisco router that runs Cisco IOS Release 12.2(7a) or another release when the global address space in the router overlaps with the VRF address that is configured on a VRF interface of a connected PE router. The VRF interface of this PE router may be unreachable but end-to-end connectivity may not be affected.

  Workaround: There is no workaround.

- CSCdz84583

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCec76965

  Symptoms: When configuring QoS on a Cisco 7200 series router that is running the c7200-jk9s-mz.122-17a image, the router may reload with a Bus Error. Specifically, the Bus Error will occur after having configured “no class xxx” on subinterfaces.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(17a).

Workaround: There is no workaround.

- CSCed19669

  Symptoms: Some calls experience one way voice where the caller hears nothing. The problem worsens as more time passes.

  Conditions: This problem occurs in a Cisco AS5800 that is running c5800-p4- mz.122-7d.bin and works as VoIP ingress gateway.

  Workaround: Reload DSP module.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed35253

  Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

  Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

  Workaround: Disable IP Inspect and IDS.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed45746

  Symptoms: Several prefixes for non-redistributed connected interfaces in different VRFs may be partially bound to the same MPLS-VPN label, thus disrupting traffic bound to one or more of these VRFs.

  Conditions: This symptom can occur on a Cisco router that runs Cisco IOS Releases 12.2, 12.2T, 12.0S, 12.3 after the VRF interfaces have flapped. The symptom may occur in all code levels of these releases.

  Workaround: Clear the routes in the VRFs in sequence.

- CSCed47409

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), a router may reload after accessing a freed Label Information Base (LIB) entry. When the symptom occurs, an error message similar to the following is likely to precede the reload:

  ```
  %TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13
  ```

  Conditions: This symptom is observed when a very uncommon timing of a Label Distribution Protocol (LDP) events occurs. The symptom may occur with LDP or Tagswitching Distribution Protocol (TDP).

  Workaround: There is no workaround.

- CSCed57482

  Symptoms: A Cisco router may reload unexpectedly with a bus error when under stress.

  Conditions: Dynamic crypto map is being used in this IPSec responder router with Cisco IOS Release 12.2(any). Router is under stress and/or number of established IPsec tunnels reached the HW engine's flow limit.

  This crash is not seen with Cisco IOS Releases 12.2 T, 12.3, or 12.3 T but only with Release 12.2.

  Workaround: Use static crypto maps instead of dynamic crypto maps. Lower the stress level and/or number of IPsec tunnels.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

- CSCed83744

  Symptoms: One way audio issues are observed in a network.

  Conditions: This symptom is observed on a Cisco AS5800 series universal gateway.

Workaround: There is no workaround.

- CSCed93836

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCin65147

  Symptoms: A VC that is configured on an IMA interface may remain in the inactive state.

  Conditions: This symptom is observed when the VC is in the inactive state while the links come up. In this situation, the VC should enter the “up” state, but does not do so.

  Workaround: Remove and reconfigure the VC.

- CSCin68517

  Symptoms: A Cisco router that is running Cisco Gateway GPRS Support Node (GGSN) software may show high CPU usage if deletion of a lot of PDP contexts is initiated from the GGSN side.

  Conditions: Such deletion of a lot of PDPs from GGSN can be initiated from GGSN when the **clear** command is issued for all PDPs or all PDPs of a path/apn etc., or, if the update request is received on a path with a different restart count at a point when the path has lot of PDP contexts belonging to it.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(23)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(23). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(23). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCec17234

  Symptoms: A PC that is running Tactical Software DialOut/EZ software may halt data transfer.

  Conditions: This symptom is observed with Tactical Software DialOut/EZ software that is running on a PC and a modem that is attached to a Cisco AS5300 that is running Cisco IOS software. The Cisco IOS software may lower the Data Set Ready (DSR) Data Carrier Detect (DCD) with a Clear To Send (CTS) message to the PC side. This causes the PC to halt data transfer.

  Workaround: There is no workaround.

- CSCec25430

  Symptoms: When you reload a faulty Cisco IP Conference Station 7935, a Catalyst 4000 Supervisor Engine III or IV may reload. Before the supervisor engine reloads, the following message may be displayed:

  ```
  %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
  duplex), with SEP00e0752447b2 port 1 (half duplex).
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 4000 Supervisor Engine III or IV that runs Cisco IOS Release 12.1(19)EW1. The symptom may also occur in other releases.

  Workaround: Disconnect the Cisco IP Conference Station 7935 or disable Cisco Delivery Protocol (CDP) by entering the **no cdp enable** interface configuration command.

- CSCec39376

  Symptoms: A Flash memory card may become corrupted. The output of the **show** *flash-filesystem* EXEC command may display the following information:

  ```
  Open device slot0 failed (Bad device info block)
  ```

  Conditions: This symptom is observed on a Cisco platform when you perform an online insertion and removal (OIR) of the Flash memory card.

  Workaround: Do not perform an OIR of the Flash memory card. Rather, switch off the router and perform an offline insertion and removal.

  If the Flash memory card does become corrupted after an OIR, reformat the Flash memory card.

- CSCec43286

  Symptoms: A Cisco router may fail to process Cisco Discovery Protocol (CDP) packets and update the IP process for On Demand Routing (ODR) routes.

  Conditions: This symptom is mainly observed on WAN interfaces with traffic that is passing through the link when a Cisco router fails to update the hold-down timer and the IP process when it receives a CDP packet from a neighbor.

  Workaround: There is no workaround.

- CSCec47615

  Symptoms: A Service Assurance Agent (SAA) version 2.2.0 Response Time Reporter (RTR) jitter probe may fail because of a timeout, Packet Missing in Action (MIA) condition, and internal error.

  Some combinations of jitter probe options such as “num-packets,” interval, “request-data-size,” and frequency may not function either.

  Conditions: This symptom is observed when the “type udpEcho” RTR responder option is configured.

  Workaround: Only configure RTR responder, that is, without the “type udpEcho” option.

- CSCec85347

  Symptoms: A Cisco 3660 that runs Cisco IOS Release 12.2(13c) may reload unexpectedly because of memory corruption.

  Conditions: This symptom is observed on a Cisco 3660 but may occur also on other platforms that run Cisco Release 12.1 E, 12.2, or 12.2 S. The symptom occurs under the following conditions:

  – Connection accounting is enabled on the router.
  – The router operates under stress.
  – An illegal write operation is performed on "BLOCKMAGIC" by the authentication, authorization, and accounting (AAA) accounting process.

  Workaround: Disable connection accounting.

  Note that the symptom does not occur in Cisco IOS Release 12.3. Impacts 12.2T versions prior to 12.2(4)T.

EXEC and Configuration Parser

- CSCec70956

  Symptoms: The command confirmation procedure in Cisco IOS software allows any word that starts with the letter "y" ("yeah," "yea," and so on) for confirmation and any word that starts with the letter "n" ("nope," "nep," and so on) for rejection.

  This situation may lead to the erasure of critical information, for example, when you do not enter an explicit "no" as a rejection after you have entered the **copy tftp: startup-config** privileged EXEC command and the following warning and user prompt for confirmation is displayed:

  ```
  % Warning: Saving this config to nvram may corrupt any network management or security
  files stored at the end of nvram.

  Continue? [no]:
  ```

  Note that the symptom is not specific to the behavior of the **copy tftp: startup-config** privileged EXEC command copy command but relates to the command confirmation procedure that is used in Cisco IOS software.

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround. The fix for this caveat ensures that only an explicit "yes" is accepted for confirmation and only an explicit "no" is accepted for rejection in the Cisco IOS command confirmation procedure.

IBM Connectivity

- CSCec86476

  Symptoms: During the configuration of a serial interface that is connected to a peer, a router may reload unexpectedly because of a software condition when you enter packet sizes for the *in-size* and *out- size* arguments of the **x25 pvc** *circuit* **qllc** *x121- address* **packetsize** *in-size out- size* interface configuration command that are smaller than the packets sizes for the *in-size* and *out-size* arguments of the **x25 facility packetsize** *in-size out-size* interface configuration or s.25 profile configuration command.

  Conditions: This symptom is platform independent and has been observed in Cisco IOS Release 12.2(15)T8 and 12.3(3a) but may also occur in other releases.

Temporary Workaround: On the router and its peers, enter packet sizes for the *in-size* and *out-size* arguments of the **x25 pvc** *circuit* **qllc** *x121-address* **packetsize** *in-size out-size* interface configuration command that are larger than the packets sizes for the *in-size* and *out-size* arguments of the **x25 facility packetsize** *in-size out-size* interface configuration or s.25 profile configuration command.

This workaround is temporary, because after the router reloads, you must apply the workaround again.

Interfaces and Bridging

- CSCea59948

  Symptoms: A cbus complex (which will bring down all the interfaces on the box for some time but the router will not reload) may be observed on a Cisco router when the following message appears on the serial interface:

  %RSP-3-RESTART: interface Serial8/1/0/23:23, not transmitting

  Conditions: This symptom occurs specifically on a Cisco 7500 series router when Multilink PPP (MLP) is configured on the serial interface and distributed Cisco Express Forwarding (dCEF) switching is enabled.

  The problem occurs when multilink member links flap. It may be after a single flap or multiple flaps.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeb04048

  Symptom: An Open Shortest Path First (OSPF) interface may be reported to be in the “down” state while the interface and the line protocol may be reported to be in the “up” state. This situation causes missing OSPF neighbor adjacencies on the OSPF interface that is in the “down” state.

  Condition: This symptom is observed when there are a large number of active interfaces and one of the following events has occurred:

  – You have upgraded a Cisco IOS image on a Route Processor (RP).
  – You have reloaded a RP.
  – You have reloaded microcode onto a line card.
  – You have reloaded microcode onto an RP.
  – You have reloaded microcode onto both a line card and an RP.

  Workaround: Use one of the following methods to recover the OSPF interface:

  – Enter the **clear ip ospf process** privileged EXEC command.
  – Enter the **clear ip route** *network* [*mask*] EXEC command, in which the *network* [*mask*] argument is the IP address of the OSPF interface that is in the “down” state.
  – Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the OSPF interface that is in the “down” state.

- CSCec70428

  Symptoms: When Protocol Independent Multicast (PIM) dense mode is enabled, an interface in the outgoing interface list may indicate that it is in forwarding mode but the P flag may still be set to the source, group (S,G) state, preventing the interface from forwarding any packets.

  Conditions: This symptom is observed when an interface enters the forwarding mode because the prune timer expires and when there is an Internet Group Management Protocol (IGMP) member on this interface.

  Workaround: Enter the **clear ip mroute** *group* privileged EXEC command.

- CSCec72958

  Symptoms: A Cisco router that is configured for Network Address Translation (NAT) may reload unexpectedly because of a software condition.

  Conditions: This symptom is observed when the router translates a Lightweight Directory Access Protocol (LDAP) packet.

  Workaround: There is no workaround.

- CSCed10653

  Symptoms: A Cisco 2600 series may not reinstall a Fast Ethernet (FE) interface in the outgoing interface list (OIL) for multicast routes after the interface has flapped.

  Conditions: This symptom is observed a Cisco 2600 series but may occur also on other platforms. The symptom occurs when the router has the **ip igmp static-group** *group-address* interface configuration command enabled on the FE interface and when the FE interface contains a particular third-party vendor chip.

  Workaround: To reinstall the interface in the OIL, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the FE interface.

  Alternate Workaround: To reinstall the interface in the OIL, enter the **clear ip mroute** *group* privileged EXEC command.

Miscellaneous

- CSCdv10203

  Symptoms: Multicast may be disabled on an interface of a Cisco 7500 series Gigabit Ethernet Interface Processor (GEIP) or GEIP plus (GEIP+).

  Conditions: This symptom is observed when the Cisco IOS image is loaded and the configuration is added. The symptom does not occur when the configuration is added, saved, and then the Cisco IOS image is loaded.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCdv26152

  Symptoms: A DS3/E3 ATM network module may not be recognized.

  Conditions: This symptom is observed on a Cisco 3660 router after you have performed an online removal and insertion (OIR) of the DS3/E3 ATM network module.

  Workaround: Reload the router.

- CSCdv68743

  Symptoms: The performance of a router may be lower than you would expect, and CPU utilization may be high during packet forwarding.

  Conditions: These symptoms are observed on a nondistributed Cisco router that runs Cisco IOS Release 12.2, 12.2 S, 12.2 T, 12.3, or 12.3 T under the following circumstances:

  – The router has a service policy attached to one or more interfaces.
  – The policy map of the service policy contains one or more class maps that are configured with one or more **match access-group name** *access-group-name* class-map configuration commands.
  – There is a large number of named extended IP access control list (ACLs) configured on the router, and the packets that are passing through the router match these ACLs.

  Workaround: If this is an option, enter the **match access-group** *access-group* class-map configuration command in the class maps, that is, enter the *access-group* argument instead of the *access-group-name* argument.

- CSCdy69194

  Symptoms: A Cisco Versatile Interface Processor (VIP) may reload after a software upgrade.

  Conditions: This symptom is observed on a Cisco 7500 series that has a VIP 2-50 in which two single-port Fast Ethernet port adapters are installed. The symptom occurs after the Cisco 7500 series is upgraded from Cisco IOS Release 12.1(2) to Release 12.1(16). The symptom may also occur with other Cisco IOS releases.

  Workaround: Set the single Fast Ethernet interface or both Fast Ethernet interfaces to be administratively shut down while the router boots up with the new Cisco IOS release. The interfaces can be brought back up individually after the software is loaded and the router is stable.

- CSCdz64323

  Symptoms: A Cisco router may reload because of a software condition when it receives a certificate revocation list (CRL) from an Lightweight Directory Access Protocol.(LDAP) server during the certificate validation process.

  Conditions: This symptom is observed on a Cisco 7200 series but may also occur on other Cisco routers.

  Workaround: There is no workaround.

- CSCea13771

  Symptoms: A Cisco uBR7100 series may reload and generate the following error message:

  ```
  %SYS-2-INTSCHED: "suspend" at level 4
  ```

  Conditions: This symptom is observed on a Cisco uBR7100 series but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCea29640

  Symptoms: A 1-port High-Speed Serial Interface network module (NM-1HSSI) that is running Frame Relay traffic shaping (FRTS) and Frame Relay fragmentation 12 (FRF.12) may randomly stop functioning and does not recover on its own. This problem is not limited to FRF.12 and could happen with other configurations also.

  Conditions: This symptom is observed on a Cisco 3600 router that is running Cisco IOS Release 12.2(11)T1 or Release 12.2(13a).

  Workaround: Disabling FRF.12 fragmentation might help.

First Alternate Workaround: Enter the **clear interface** EXEC command on the affected interface.

Second Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCea47284

  Symptoms: CPUHOG messages and tracebacks may occur on a Cisco router when you attempt to register more than 10,000 gateways.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Processing Engine G1 (NPE-G1).

  Workaround: There is no workaround.

- CSCea59073

  Symptoms: Downloading a certificate revocation list (CRL) through a Simple Certificate Enrollment Protocol (SCEP) GetCRL action may fail and may cause the router to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router when there is no CRL distribution point (CDP) included in the certificate.

  Workaround: If this is an option, use a CDP.

- CSCea63499

  Symptoms: A Cisco 7200 may reload unexpectedly when it attempts to translate virtual address 0x3C0C00C0 to a physical address.

  Conditions: This symptom is observed under rare conditions on a Cisco 7200 that is configured with a C7200-I/O-FE I/O controller in slot 0. The symptom is related to an error in the Fast Ethernet controller on the I/O controller.

  Workaround: There is no workaround.

- CSCea74331

  Symptoms: A Cisco 7200 series or Cisco uBR7200 series may reload unexpectedly when you perform an online insertion and removal (OIR) of a 2-port multichannel T3 port adapter (PA-MC-2T3).

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco uBR7200 series that run Cisco IOS Release 12.2 when the interfaces of the PA-MC-2T3 are configured for PPP encapsulation. The symptom may occur also in other releases.

  Workaround: There is no workaround.

- CSCeb52270

  Symptoms: An interface of a Cisco router may not be able to receive traffic that is destined for an address that is configured on the router.

  Conditions: This symptom is platform independent and occurs only when there is a route in a different VPN routing and forwarding instance (VRF) that is attached or connected to the interface. This may occur when the route has been exported from one VRF to another or when a static route in a VRF points to the interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCeb59201

  Symptoms: A start accounting request is not sent for a redundant dial peer when the primary dial peer fails.

Conditions: This symptom is observed on a Cisco AS5300.

Workaround: There is no workaround.

- CSCeb66825

  Symptoms: A Cisco 7200 series may reload unexpectedly during a service-policy configuration.

  Conditions: This symptom is observed when you attach a level 2 policy map as a child of a level 1 policy map and when the level 1 policy map is already attached to an interface.

  Workaround: Create a level 3 policy map, and attach it to the interface.

- CSCec00268

  Symptoms: A multilink interface may stop processing received packets.

  Conditions: This symptom is observed on a Cisco 7500 series when Multilink PPP (MLP) is configured and when a lot of traffic is forwarded to the process-switching path.

  Workaround: To clear the symptom, move the physical interfaces to a new multilink interface with a new interface number.

- CSCec06146

  Symptoms: A serial interface of a 1-port multichannel E3 port adapter (PA-MC-E3) may fail to enter the "up/up" state when you initially configure the interface or after a number of reconfigurations.

  Conditions: This symptom is observed on a PA-MC-E3 that is installed in a Cisco 7500 series or Cisco 7600 series when the following sequence of events occurs:

  1. You configure an interface by entering the **controller e3** *slot/port* global configuration command followed by the **e1** *line-number* **channel-group** *channel* **timeslots** *range* controller configuration command.

  2. You delete the interface by entering the **controller e3** *slot/port* global configuration command followed by the **no e1** *line-number* **channel-group** *channel* controller configuration command.

  3. You reconfigure the interface by entering the commands listed in Step 1.

  Although the symptom may occur when you initially configure the interface, it is more likely to occur when you configure, delete, and reconfigure the interface several times.

  Workaround: When the interface does not enter the "up/up" state, configure the interface again.

- CSCec06275

  Symptoms: The following error message may be displayed on the console of a Route Switch Processor (RSP):

  ```
  %CBUS-3-CMDDROPPED: Cmd dropped,CCB 0xF800FFB0,slot 9, cmd code 24
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when software compression is enabled on serial interfaces and dialer interfaces and when Cisco Express Forwarding (CEF) switching rather than distributed CEF (dCEF) switching is enabled. This situation causes software compression to occur on the RSP.

  Because software compression is enabled on all the serial interfaces, the CPU utilization of the RSP becomes very high, causing commands to be dropped.

  Workaround: Remove software compression from the serial interfaces.

- CSCec06341

  Symptoms: A Cisco router may reload unexpectedly because of memory corruption with a corrupted redzone without any intervention.

Conditions: This symptom is observed on a Cisco router when multicast traffic is protected by an IP Security (IPSec) generic routing encapsulation (GRE) tunnel.

Workaround: There is no workaround.

- CSCec11122

  Symptoms: A Cbus Complex may occur and the packet memory may be recarved, causing a temporary disruption in service.

  Conditions: This symptom is observed on a Cisco 7500 series when you install an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) or an enhanced 2-port T1/E1 high-capacity port adapter (PA-VXC-2TE1+) and when you configure the port adapter via the command-line interface (CLI) for E1 or T1.

  Workaround: There is no workaround. Try to install the port adapter during a maintenance window.

- CSCec15598

  Symptoms: While running Cisco IOS Release 12.2(17a), a Cisco 3640 router may run out of processor memory due to a memory leak in the TCL IVR process.

  Conditions: This symptom occurs under the following conditions: - Only when using Interactive Voice Response (IVR) - When E1 R2 signaling is configured - When a TCL IVR 1.0 script is used - Only when DISCONNECT messages arrive with a PI value

  Workaround: The memory leak is not present in Cisco IOS Release 12.2(6).

- CSCec25317

  Symptoms: A Versatile Interface Processor 4 (VIP4) in which an 8-port multichannel E1, G.703 120 ohm interface port adapter (PA-MC-8E1/120) is installed may reload unexpectedly and display the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address.
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that has a distributed multilink interface on which IP Header Compression (IPHC) is configured when distributed Cisco Express Forwarding (dCEF) is disabled by entering the **no ip cef distributed** global configuration command and reconfigured by entering the **ip cef distributed** global configuration command while the interface is operational.

  Workaround: Ensure that the multilink interface is shut down before you to disable dCEF.

- CSCec26539

  Symptoms: A Cisco router that has a Hot Standby Router Protocol (HSRP) group configured on a subinterface may stop responding and may reload.

  Conditions: This symptom is observed when an HSRP Simple Network Management Protocol (SNMP) query is performed. The symptom occurs only when HSRP is configured on a subinterface. The symptom does not occur for an HSRP group that is configured on a major interface.

  Workaround: Do not initiate an SNMP query for HSRP.

  Alternate Workaround: Use the **snmp-server** global configuration command to specify which MIBs are available (for example):

  snmp-server view HSRP internet included snmp-server view HSRP ciscoHsrpMIB excluded snmp-server view HSRP ciscoHsrpExtMIB excluded snmp-server community public view HSRP RW 20 snmp-server community private view HSRP RW 20

- CSCec29430

  Symptoms: The Systems Network Architecture switching services (SNASw) performance via single-hop Enterprise Extender (EE) Rapid Transport Protocol (RTP) connections is not optimum.

Conditions: This symptom is observed on a Cisco router that runs SNASw and that has EE High Performance Routing (HPR)/IP RTP connections. Normal (that is, non-EE) HPR-ISR RTP connections are not affected.

An RTP connection has an alive timer that comes up every 180 seconds when there is no traffic. An EE RTP connection has also an underlying Logical Data Link Control (LDLC) timer that can detect problems with the EE link. For these EE RTP connections, the RTP alive timer is not required when the RTP path is limited to a single hop (or to two hops through a virtual routing node); the LDLC timer is sufficient.

Workaround: There is no workaround. The fix for this caveat disables the RTP alive timer for single-hop EE RTP connections, thereby improving the SNASw performance.

- CSCec31162

  Symptoms: Incorrect tags may be imposed after a route has flapped.

  Conditions: This symptom is observed on a Cisco router that functions in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment.

  Workaround: There is no workaround.

- CSCec32135

  Symptoms: When **set** commands are used with a service policy, a router may reload unexpectedly. In particular, when you use the **set cos** policy-map class configuration command, a router may reload unexpectedly.

  Conditions: This symptom is observed when you make a configuration change of a service policy that is configured on an interface, when the service policy is configured with a **set** command, and when one or all of the following three features are enabled:

  - access control list (ACL) filtering

  - unicast Reverse Path Forwarding (uRPF)

  - multicast routing

  Workaround: There is no workaround.

- CSCec39685

  Symptoms: A router that runs Voice over IP (VoIP) may reload frequently during the authentication, authorization, and accounting (AAA) process when there is an accounting attribute with an invalid length such as a zero-length user name and when too many attributes are sent to the AAA server.

  Conditions: This symptom is observed on a Cisco 3660 router that runs Cisco IOS Release 12.2(19). The symptom may also occur in other releases. The condition that causes VoIP to send a zero-length user name is unknown, and is documented in caveat CSCec52917.

  Workaround: There is no workaround.

- CSCec48611

  Symptoms: A Cisco voice gateway may report IP and telephony call legs that remain active even though the calls are no longer active.

  Conditions: This symptom is observed on a Cisco AS5400HPX voice gateway that is running Cisco IOS Release 12.2(11)T under high CPU utilization. In addition, the gateway uses the interactive voice response (IVR) 2.0 session application to handle blind call transfers. The symptom may occur also in other releases.

  Workaround: There is no workaround.

- CSCec52123

  Symptoms: A Cisco 2600 series or Cisco 3600 series may generate badshare messages.

  Conditions: This symptom is observed on a Cisco 2600 series and Cisco 3600 series that are configured with a compression Advanced Integration Module (AIM) and an 8-port asynchronous/synchronous network module (NM-8A/S).

  Workaround: Use software compression instead of hardware compression.

- CSCec57190

  Symptoms: Output drops may occur and increase on interfaces that have weighted fair queuing (WFQ) enabled by default.

  Conditions: This symptom is tied specifically to a Cisco 7200 series that is configured with a Network Service Engine 1 (NSE-1) and a Cisco 7401 that have Parallel Express Forwarding (PXF) enabled and that are using a default hold-queue size.

  Workaround: Configure an output hold-queue size on the interface by entering the **hold-queue** *length* **out** interface configuration command. Note that this workaround does not apply to Cisco IOS Release 12.2.

  First Alternate Workaround: Disable PXF by entering the **no ip pxf** global configuration command.

  Second Alternate Workaround: Disable WFQ by entering the **no fair-queue** interface configuration command.

- CSCec63438

  Symptoms: The **set** command does not work when you use the command in a non-leaf level in a hierarchical policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) but may also occur in other releases.

  Workaround: There is no workaround.

- CSCec86102

  Symptoms: Tag entries may be missing on a Versatile Interface Processor (VIP).

  Conditions: This symptom is observed on a Cisco 7500 series that has distributed Cisco Express Forwarding (dCEF) enabled.

  Workaround: Enter the **clear cef linecard** user EXEC or privileged EXEC command.

- CSCed09364

  Symptoms: Ping packet that are larger than 1498 bytes may not pass successfully through a multilink interface.

  Conditions: This symptom is observed when a bridge group is configured on a multilink interface. The symptom does not occur when there is no bridge group on the multilink interface.

  Workaround: Change the maximum transmission unit (MTU) on the multilink interface from the default value of 1500 bytes to 1498 bytes.

- CSCed19065

  Symptoms: A session may not be set up correctly, or the session is set up but you cannot send any data via the session.

  Conditions: This symptom is observed when a Primary Logical Unit (PLU) name that is presented by a Dependent Logical Unit Requestor (DLUR) to a Secondary Logical Unit (SLU) in a BIND request is not the same as the PLU name that is received in an INIT-SELF request. The PLU name

in the INIT-SELF request may consist of four characters followed by four blanks (a total of eight characters), but the PLU name in the BIND request may consist of only four characters without any blank padding at the end of the name.

Workaround: Modify the PLU name that is received in the BIND request so that the name consists of eight characters.

- CSCed22837

  Symptoms: A router may reload unexpectedly when packets are tag switched.

  Conditions: This symptom is observed when a Bridge-Group Virtual Interface (BVI) is created after the router has booted up, when IP packets are received through the BVI, and when these IP packets are forwarded as Multiprotocol Label Switching (MPLS) packets through another interface.

  Workaround: Disable tag switching on the BVI interface by entering the **tag-switching ip** interface configuration command followed by the **no tag-switching ip** interface configuration command.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCuk47528

  Symptoms: Packet redirection to a cache may not occur even though Web Cache Communication Protocol (WCCP) is enabled and the cache farm has formed successfully. The symptom may be invisible to end users because packets (usually packets that are part of HTTP sessions) still flow successfully to and from their original destinations.

  Conditions: This symptom is observed on a Cisco platform when both WCCP and Cisco Express Forwarding (CEF) are enabled.

  Workaround: Disable CEF on all interfaces on which a WCCP redirect statement is configured.

TCP/IP Host-Mode Services

- CSCdx95455

  Symptoms: A memory leak may occur on a router after TCP-to-X.25 translation is configured.

  Conditions: This symptom is observed if a user attempts to use TCP-to-X.25 translation while a router is already performing translation for the maximum number of configured users. The additional user will not be able to use translation, and the router will leak memory.

  Workaround: There is no workaround.

- CSCeb54456

  Symptoms: A Data-link switching plus (DLSw+) circuit may not function when a TCP connection gets stuck. After about 90 seconds, the TCP connection is closed by DLSw+, and a new TCP connection is built for DLSw+. Once the new TCP connection is up, the DLSw+ circuit starts functioning again.

  Conditions: This symptom is observed on a Cisco router that is configured with both a DLSw+ interface and an ATM interface.

  Possible Workaround: I this is an option, remove the ATM interface from the router. When you configure the DLSw+ interface and the ATM interface on different routers, the symptom does not occur.

Wide-Area Networking

- CSCec15600

  Symptoms: An input queue of an interface may become wedged, and the output of the **show buffers input-interface** EXEC command may not display any packets.

  Conditions: This symptom is observed on a Cisco 7500 that is configured with dialer interfaces and a service policy.

  Temporary Workaround: Increase the input hold queue.

- CSCec41364

  Symptoms: A Cisco IOS Network Access Server (NAS) may send incorrect port information in accounting records.

  Conditions: This symptom is observed when performing callback without peer authentication.

Workaround: There is no workaround.

- CSCec68292

  Symptoms: Dialer ping packets that are transferred via an asynchronous line may be dropped at the receiving end.

  Conditions: This symptom is observed on a Cisco platform when the interface at the receiving end has the **dialer map** interface configuration command enabled.

  Workaround: Do not enter the **dialer map** interface configuration command. Rather, enter the **dialer string** interface configuration command.

- CSCec72974

  Symptoms: A router may not reestablish the backup connection when an active physical ISDN link is interrupted.

  Conditions: This symptom is observed on a Cisco router that has dialer backup configured using the Dialer Watch feature. Note that the symptom does not occur when the **debug dialer events** privileged EXEC command is enabled.

  Workaround: To ensure that there is always one B channel available for dialup, even when the ISDN link toggles and causes and active call to be terminated, enter 1 for both the minimum and maximum arguments in the **dialer pool-member** *number* **min-link** *minimum* **max-link** *maximum* interface configuration command.

  Alternate Workaround: Enter the **debug dialer events** privileged EXEC command.

Resolved Caveats—Cisco IOS Release 12.2(21b)

Cisco IOS Release 12.2(21b) is a rebuild release for Cisco IOS Release 12.2(21). The caveats in this section are resolved in Cisco IOS Release 12.2(21b) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCdz32659

  Symptoms: Many memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of
  -1732547824 bytes failed from x605111F0, pool Processor, alignment 0
  -Process= "CDP Protocol", ipl= 0, pid= 42
  -Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  Conditions: The symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(17)ST. The symptom may also occur on other Cisco 7500 series routers that run Release 12.0 S, 12.2 S, 12.3, or 12.3 T.

  Workaround: To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCin67568

  Symptoms: A Cisco Catalyst 2950 experiences a memory leak in the CDP process.

  Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

  Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

Miscellaneous

- CSCdy40928

  Symptoms: Connectivity difficulties may occur when Virtual Private Network (VPN) routing/forwarding (VRF) packets follow the global routing table instead of the VRF table.

  Conditions: This symptom is observed on a low-end Cisco router that runs Cisco IOS Release 12.2(7a) or another release when the global address space in the router overlaps with the VRF address that is configured on a VRF interface of a connected PE router. The VRF interface of this PE router may be unreachable but end-to-end connectivity may not be affected.

  Workaround: There is no workaround.

- CSCdy69194

  Symptoms: A Cisco Versatile Interface Processor (VIP) may reload after a software upgrade.

  Conditions: This symptom is observed on a Cisco 7500 series that has a VIP 2-50 in which two single-port Fast Ethernet port adapters are installed. The symptom occurs after the Cisco 7500 series is upgraded from Cisco IOS Release 12.1(2) to Release 12.1(16). The symptom may also occur with other Cisco IOS releases.

  Workaround: Set the single Fast Ethernet interface or both Fast Ethernet interfaces to be administratively shut down while the router boots up with the new Cisco IOS release. The interfaces can be brought back up individually after the software is loaded and the router is stable.

- CSCdz84583

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCea63499

  Symptoms: A Cisco 7200 may reload unexpectedly when it attempts to translate virtual address 0x3C0C00C0 to a physical address.

  Conditions: This symptom is observed under rare conditions on a Cisco 7200 that is configured with a C7200-I/O-FE I/O controller in slot 0. The symptom is related to an error in the Fast Ethernet controller on the I/O controller.

  Workaround: There is no workaround.

- CSCeb22276

  Symptoms: Some Simple Network Management Protocol (SNMP) packets may linger in the input queue while they are processed. However, the packets do exit the queue on their own without any intervention from the user. This fix allows these packets to be removed from the queue more quickly.

  Conditions: This symptom is observed on a device that runs Cisco IOS software and that supports SNMP operations. In addition, the SNMP request must contain a valid community string.

  Workaround: Protect the SNMP community strings with good password management. Permit SNMP traffic only from trusted devices.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed35253

  Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

  Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

  Workaround: Disable IP Inspect and IDS.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending

upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed45746

  Symptoms: Several prefixes for non-redistributed connected interfaces in different VRFs may be partially bound to the same MPLS-VPN label, thus disrupting traffic bound to one or more of these VRFs.

  Conditions: This symptom can occur on a Cisco router that runs Cisco IOS Releases 12.2, 12.2T, 12.0S, 12.3 after the VRF interfaces have flapped. The symptom may occur in all code levels of these releases.

  Workaround: Clear the routes in the VRFs in sequence.

- CSCed47409

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), a router may reload after accessing a freed Label Information Base (LIB) entry. When the symptom occurs, an error message similar to the following is likely to precede the reload:

  ```
  %TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13
  ```

  Conditions: This symptom is observed when a very uncommon timing of a Label Distribution Protocol (LDP) events occurs. The symptom may occur with LDP or Tagswitching Distribution Protocol (TDP).

  Workaround: There is no workaround.

- CSCed57482

  Symptoms: A Cisco router may reload unexpectedly with a bus error when under stress.

  Conditions: Dynamic crypto map is being used in this IPsec responder router with Cisco IOS Release 12.2(any). Router is under stress and/or number of established IPsec tunnels reached the HW engine's flow limit.

  This crash is not seen with Cisco IOS Releases 12.2 T, 12.3, or 12.3 T but only with Release 12.2.

  Workaround: Use static crypto maps instead of dynamic crypto maps. Lower the stress level and/or number of IPsec tunnels.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

- CSCin68517

  Symptoms: A Cisco router that is running Cisco Gateway GPRS Support Node (GGSN) software may show high CPU usage if deletion of a lot of PDP contexts is initiated from the GGSN side.

  Conditions: Such deletion of a lot of PDPs from GGSN can be initiated from GGSN when the **clear** command is issued for all PDPs or all PDPs of a path/apn etc., or, if the update request is received on a path with a different restart count at a point when the path has lot of PDP contexts belonging to it.

  Workaround: There is no workaround.

- CSCed93836

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Resolved Caveats—Cisco IOS Release 12.2(21a)

Cisco IOS Release 12.2(21a) is a rebuild release for Cisco IOS Release 12.2(21). The caveats in this section are resolved in Cisco IOS Release 12.2(21a) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCec28873

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCec85347

  Symptoms: A Cisco 3660 router that is running Cisco IOS Release 12.2(13c) may experience a memory corruption crash.

  Conditions: This crash is due to an illegal write on BLOCKMAGIC by the AAA accounting process. The crash is seen under stress conditions with connection accounting configured on the router.

  Workaround: Turn off connection accounting.

- CSCec86420

  Symptoms: When you enter the **undebug all** privileged EXEC command on a Cisco 3700 series, all traffic that passes through an encrypted generic routing encapsulation (GRE) tunnel may stop.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured with a GRE tunnel that is secured via IP Security (IPSec) and that is using Cisco Express Forwarding (CEF) switching.

  Workaround: Reinitialize CEF switching by entering the **no ip cef** global configuration command followed by the **ip cef** global configuration command.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Resolved Caveats—Cisco IOS Release 12.2(21)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(21). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(21). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCea74631

  Symptoms: A Route Switch Processor (RSP) that is acting as a slave may have complete packet switching activity interrupted for several minutes. This situation may cause the RSP to permanently pause.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(12d).

  Workaround: There is no workaround.

- CSCec03906

  Symptoms: Packets will be rejected when nontransparent text is received and the block check character (BCC) is 0x7f.

  Conditions: This symptom is observed when a Cisco 1600 series runs in bisynchronous mode with the ASCII character set.

  Workaround: There is no workaround.

- CSCec17234

  Symptoms: A PC that is running Tactical Software DialOut/EZ software may halt data transfer.

  Conditions: This symptom is observed with Tactical Software DialOut/EZ software that is running on a PC and a modem that is attached to a Cisco AS5300 that is running Cisco IOS software. The Cisco IOS software may lower the Data Set Ready (DSR) Data Carrier Detect (DCD) with a Clear To Send (CTS) message to the PC side. This causes the PC to halt data transfer.

  Workaround: There is no workaround.

- CSCec25430

  Reloading a faulty Cisco IP conference station 7935 may cause a Catalyst 4000 sup III/IV to reload. Prior to the supervisor reloading the following message may be seen:

  ```
  %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
  duplex), with SEP00e0752447b2 port 1 (half duplex).
  ```

  Workaround: Disconnect the 7935 phone or disable CDP.

  switch(config-if)#**no cdp enable**

IBM Connectivity

- CSCea86421

  Symptoms: The focal point buffer may overflow as shown in the following messages:

  ```
  SNA: MV_SendVector rc = 8001
  SNA: Alert E14A3440 not sent, Focal point buffer overflowed
  ```

  In the latter message the Alert ID (E14A3440) may vary.

  Conditions: This symptom is observed on a Cisco router that has a Systems Network Architecture (SNA) physical unit (PU) that is defined with a focal point.

  Workaround: Remove the SNA PU definitions from the router and configure them again.

- CSCec02827

  Symptoms: Data-link switching (DLSw) Synchronous Data Link Control (SDLC) receives a Null XID Command and responds back with another Null XID Command. It should be a Null XID Response. The DLSw circuit never goes into the CONNECTED state but stays in the CKT_ESTABLISHED state until it drops.

  Further Problem Description:

  The Ethernet attached Tandem physical unit (PU) 2.0 attempts to establish a session via DLSw to SDLC where the DLSw SDLC interface is running role secondary. The PU 2.0 sends in a Null XID Command but DLSw / SDLC responds with another Null XID Command instead of sending a Null XID Response. The SDLC interface is constantly receiving Set Normal Response Mode (SNRM) from the SDLC primary device but will not respond with an unnumbered acknowledgement (UA)

until it receives a "real" XID from the PU 2.0. A "real" XID is a nonnull XID with a length 3 or more. But, the Tandem's finite state machines (FSM) will not transition to send the "real" XID until it receives a Null XID Response. Additional Information:

A **show DLSw circuits** [**detail**] privileged EXEC command shows the circuit in the CKT_ESTABLISHED state with a large number of XIDs both sent and received. A **show interfaces serial x/y** EXEC command shows the following:

```
sdlc addr xx state is SNRMSEEN
cls_state is CLS_FULL_XID_PEND
```

Conditions: This symptom is observed on Cisco platforms that are running Cisco IOS software.

Workaround: There is no workaround.

- CSCec10234

  Symptoms: Ethernet redundancy may not function with Inter-Switch Link (ISL) trunking.

  Conditions: This symptom is observed on a Cisco router or switch that is configured for data-link switching (DLSw) and Ethernet Redundancy (ER).

  Workaround: There is no workaround.

- CSCec24088

  Symptoms: A Cisco router that is configured for data-link switching (DLSw) may generate the following error messages and tracebacks:

```
%TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps pointer: 0x0
-Process= "DLSw Peer Process", ipl= 0, pid= 81
-Traceback= 603BDCDC 603BEFC4 60AC5A24 60AC6E00 60AC4F54 60AB51D0 60AB4D04 60AB4 958
60223B44 60223B30
%TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps pointer: 0x0
-Process= "IP Input", ipl= 0, pid= 29
-Traceback= 603BDCDC 603BEFC4 60AC5A24 60AC6E00 60AC4F54 60AB51D0 60ABCF44 603BD C28
60325EC0 60327C44 6035E49C 60346DCC 603452C8 603453C4 60345538 60223B44
```

  Conditions: This symptom is observed in a DLSw border peer network that uses DLSw priority peers. Note that the symptom does not affect the DLSw functionality.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCeb60620

  Symptoms: A Cisco Route Switch Processor (RSP) that is configured as a bridge may not pass bridged traffic, regardless of the protocols that are configured on Ethernet interfaces. This situation can lead to a loss of connectivity.

  Conditions: This symptom is observed on a Cisco RSP that is running a Cisco IOS rsp-jsv-mz image.

  Workaround: There is no workaround.

- CSCec44424

  Symptoms: A Cisco router does not respond to an Address Resolution Protocol (ARP) request, which is destined to its Hot Standby Router Protocol (HSRP) address, and the ARP request destination address is specific HSRP Virtual MAC address through Inter-Switch Link (ISL) link.

  Conditions: This symptom is observed on a Cisco 3640 router.

Workaround: Configure ARP Table statically on the device which sends ARP to HSRP address.

IP Routing Protocols

- CSCdz42920

  Symptoms: A Cisco router may reload by bus error when ip accounting is configured on the router.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.2(11)T2 after entering the **clear ip accounting** EXEC command.

  Workaround: Do not use the **clear ip accounting** EXEC command or the **show ip accounting** EXEC command.

- CSCea19236

  Symptoms: A router may reload.

  Conditions: This symptom is observed when a Border Gateway Protocol (BGP) policy list is used on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCea31201

  Symptoms: A Cisco router may reload unexpectedly because of a bus error at "ip_fast_accumulate_acctg."

  Conditions: This symptom is observed on a Cisco router that has the **ip accounting** interface configuration command enabled.

  Workaround: There is no workaround.

- CSCea81029

  Symptoms: A Cisco router may reload unexpectedly when you enter a **show** command that is related to IP multicast.

  Conditions: This symptom is observed on a Cisco router that has remained at the "more" prompt for a long period of time.

  Workaround: There is no workaround.

- CSCeb19676

  Symptoms: A Cisco 7206VXR periodically reloads when Network Address Translation (NAT) is configured and L4 Internet Locator Service (ILS) Lightweight Directory Access Protocol (LDAP) entries are translated.

  Conditions: This symptom is observed on a Cisco 7206VXR router with a Network Processing Engine (NPE-G1) that is running the c7200-is-mz image of Cisco IOS Release 12.2(16)B.

  Workaround: There is no workaround.

- CSCeb85136

  Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped.

  Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

  Workaround: There is no workaround.

- CSCeb86055

  Symptoms: A Cisco router does not receive and respond to an Address Resolution Protocol (ARP) request to its Hot Standby Routing Protocol (HSRP) address when “bridge group” is configured.

  Conditions: This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(17).

  Workaround: Make static ARP entry for an HSRP virtual MAC address to clear the problem.

- CSCec14415

  Symptoms: When next-hop-self is configured on a peer group, the next-hop calculation is only performed on the first member of the peer group, and the same next-hop value is replicated to the rest of the peers instead of calculating the next hop based on the next-hop-self configuration. The problem of wrong next-hop value on the peer group members occurs if the router is multihomed and if Border Gateway Protocol (BGP) uses those multiple interfaces to peer with the neighbors which are in the same peer group (or update group), then the same next-hop value of the leader of the peer group is used for all the members.

  Conditions: This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.3T.

  Workaround: Remove the peer groups to allow the calculation to be run for each neighbor.

  Alternate Workaround: Make sure that all the peers which are in the same peer group can be reached through a single interface and use that interface IP address, using the BGP **update-source** command, as the local peering address.

- CSCec29953

  Symptoms: A retransmission counter may not be reset when a neighbor is terminated.

  Conditions: This symptom is observed on a Cisco platform that is running Open Shortest Path First (OSPF) when the retransmission limit default (12 or 24) is added to the retransmission mechanism.

  Workaround: Clear the OSPF process by entering the **clear ip ospf process** *pid* privileged EXEC command. Then, enter the **limit retransmissions non-dc disable** router configuration command.

- CSCec32794

  Symptoms: A Cisco 3600 series router may reload with a bus error when Address Resolution Protocol (ARP) entry is aged out.

  Conditions: This symptom is observed when ARP entries have been populated and when a certain entry is being aged out.

  Workaround: There is no workaround.

- CSCec34459

  Symptoms: A memory leak may occur in the “IP Input” process on a Cisco platform, and memory allocation failures (MALLOCFAIL) may be reported in the processor pool.

  Conditions: This symptom is observed on a Cisco platform that is configured for Network Address Translation (NAT).

  Workaround: There is no workaround.

Miscellaneous

- CSCds48812

  Symptoms: A loopback route on a Virtual Private Network (VPN) routing/forwarding instance (VRF) may not be removed from the Cisco Express Forwarding (CEF) table.

  Conditions: This symptom is observed after you enter the **import map** VRF configuration submode command.

  Workaround: Use the **clear ip route vrf** *vrf-name* * EXEC command to remove the /32 receive entry from CEF.

- CSCdv10203

  Symptoms: Multicast may be disabled on an interface of a Cisco 7500 series Gigabit Ethernet Interface Processor (GEIP) or GEIP plus (GEIP+).

  Conditions: This symptom is observed when the Cisco IOS image is loaded and the configuration is added. The symptom does not occur when the configuration is added, saved, and then the Cisco IOS image is loaded.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCdx60661

  Symptoms: In a sniffer trace, the IP header checksum is incorrect and displays an incorrect IP version of 10 instead of 4.

  Conditions: This symptom is observed when IP traffic is destined out of the native (untagged) VLAN and when matching policies that rewrite the class of service (CoS) value to 5 corrupt the IP header.

  Workaround: Do not use the native VLAN.

- CSCea08050

  Symptoms: A Cisco router may reload if the **show ip access-list** *access-list-name* command is performed on an existing reflexive access-list.

  Conditions: This symptom is observed on a Cisco 3620 router that is running Cisco IOS Release 12.3(13).

  Workaround: There is no workaround.

- CSCea22843

  Symptoms: When configuring Routing Information Protocol (RIP) version 2 on a Cisco router, tracebacks may be displayed.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS software.

  Workaround: There is no workaround.

- CSCea47597

  Symptoms: Routing Information Protocol version 2 (RIPv2) routes get stuck in the routing table even if the next hop interface is down.

  Conditions: This symptom is observed when running Cisco IOS Release 12.1(11b) E4.

  Workaround: There is no workaround.

- CSCea53451

  Symptoms: A Cisco AS5850 may reload after 4 to 5 hours of operation.

Conditions: This symptom is observed on a Cisco AS5850 that is running Cisco IOS Release 12.2(15)T and that has a call load of 8 calls per second.

Workaround: There is no workaround.

- CSCea84387

  Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive.

  Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions.

  Workaround: Allow only one user at a time to enter MQC commands.

- CSCeb05672

  Symptoms: Cisco IOS Server Load Balancing (SLB) packets that are switched at the process level instead of at the Forwarding Information Base (FIB) level may be dropped by a Cisco router.

  Conditions: This symptom is observed when the virtual IP destination address is a dynamic alias, which occurs when the virtual IP destination address is a member of a subnet on the interface of a router.

  Workaround: Enable Cisco Express Forwarding (CEF) switching by entering the **ip cef** global configuration command, and enter the **ip route-cache cef** interface configuration command on the destination interface.

- CSCeb13472

  Symptoms: A basic ping fails on the port channel interface.

  Conditions: This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.2(15)T3.

  Workaround: There is no workaround.

- CSCeb32698

  Symptoms: A Cisco router may experience a software forced reload due to memory corruption with the following display of errors in the log:

  ```
  %SYS-3-BADFREEMAGIC: Corrupt free block at 62EE9C90 (magic 635472E4)
  ```

  Conditions: This symptom is observed on a Cisco 7206VXR that is running the c7200-g5js-mz image in Cisco IOS Release 12.2(16) and GGSN Release 1.4.

  Workaround: There is no workaround.

- CSCeb34203

  Symptoms: A Cisco router may experience output queue packet drops on the priority queue before the interface is congested on an E1 serial interface on a PA-MC-E3.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.1(18)E.

  Workaround: Use the tx-ring-limit interface configuration command to increase the value of the drivers transmitted on the queue. Refer to the following document for additional information:

  http://www.cisco.com/warp/customer/121/txringlimit_6142.html

- CSCeb35210

  Symptoms: A Cisco router that has a Quality of Service (QoS) service policy attached to an interface may generate memory alignment errors or reload unexpectedly because of a bus error during normal mode of operation.

Conditions: This symptom is observed when the policy map of the service policy has a set action configuration and when traffic is being processed.

Workaround: Remove the set action configuration from the policy map.

- CSCeb36929

  Symptoms: When a Cisco router is performing tag imposition, it may reload because of a bus error.

  Conditions: This symptom is observed when you create a new generic routing encapsulation (GRE) tunnel after the router has booted up and when GRE packets are received through this GRE tunnel and forwarded as Multiprotocol Label Switching (MPLS) packets.

  Workaround: Enter the **tag-switching ip** interface configuration command followed by the **no tag-switching ip** interface configuration command on the newly-created GRE tunnel interface.

- CSCeb36963

  Symptoms: VLAN class of service (Cos) bits may not be set for outgoing Multiprotocol Label Switching (MPLS) packets, although the modular QoS CLI (MQC) may indicate so.

  Conditions: This symptom is observed on a Cisco 7200 series or Cisco 7500 series that runs Cisco IOS Release 12.2, Release 12.3, or Release 12.3 B when CoS marking is applied to a VLAN subinterface. Note that traffic that is generated by the router itself receives the correct CoS for all classes.

  Workaround: There is no workaround.

- CSCeb46191

  Symptoms: When a Cisco router is configured for both internal Border Gateway Protocol (iBGP) load balancing and Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN), incorrect MPLS labels may be installed. When one of the load-balancing links flaps, connectivity may be lost between the VPN sites.

  Conditions: This symptom is observed in the Cisco IOS releases that are listed in the “First Fixed-in Version” field at the following location:

  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdy76273

  Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Disable iBGP load balancing.

- CSCeb49581

  Symptoms: A linkUp trap may not be generated on a Cisco router.

  Conditions: This symptom is observed on a Cisco 3600 series that runs Cisco IOS Release 12.2(17) but may also occur in other releases.

  Workaround: There is no workaround.

- CSCeb53422

  Symptoms: A call setup failure may occur for high-delay links with a round-trip time greater than 300 milliseconds.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(16) but may also occur in other releases.

  The call fallback subsystem hard-codes the amount of time it will wait for the response to probes to 300 milliseconds. The probes fail if the round-trip time is more than 300 milliseconds, even though the network is a high-bandwidth network.

  Workaround: There is no workaround.

- CSCeb56457

  Symptoms: PA-A3-8T1 inverse multiplexing over ATM (IMA) modules may drop packets with a certain unknown pattern.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(16).

  Workaround: There is no workaround.

- CSCeb59201

  Symptoms: A start accounting request is not sent for a redundant dial peer when the primary dial peer fails.

  Conditions: This symptom is observed on a Cisco AS5300.

  Workaround: There is no workaround.

- CSCeb63310

  Symptoms: A Cisco router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(17), later releases of Release 12.2, or Release 12.3. The interface of the router has an output service policy attached, and the **bandwidth** interface configuration command or the **fair-queue** interface configuration command is configured in the policy map attached by the **service-policy** router configuration command. The traffic is flowing through the interface at a fast rate. The router reloads under the following conditions:

  – The interface has the **ip rsvp bandwidth** interface configuration command configured, and the router reloads when you enter the **no ip rsvp bandwidth** interface configuration command.

  – The interface does not have the **ip rsvp bandwidth** interface configuration command configured, and you issue the **ip rsvp bandwidth** interface configuration command.

  – You issue the **ip rtp reserve** *lowest-udp-port range-of-ports* interface configuration command.

  In all three situations, a service policy that is configured with the **bandwidth** or **fair-queue** command is attached to the interface.

  Workaround: Shut down the interface before issuing the above commands. Enable the interface again after issuing the commands.

- CSCeb67939

  Symptoms: When an UNBIND request is received, a Systems Network Architecture (SNA) switch fails to write the Physical Unit (PU) name into the UNBIND response that is built as a result. Internal buffer corruption occurs.

  Conditions: This symptom is observed on a Cisco router that has an SNA switch.

  Workaround: There is no workaround.

- CSCeb68061

  Symptoms: In an interautonomous setup in the Autonomous System Boundary Router (ASBR), the label for a prefix in the label forwarding information base (LFIB) may be inconsistent with the actual label in the multiprotocol external Border Gateway Protocol (MP-eBGP) table.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 12.2.

  Workaround: Execute the **clear ip bgp** *neighbor-address* privileged EXEC command where *neighbor-address* is the address of the eBGP peer from which we learn the route to the prefix whose label is wrong.

- CSCeb73681

  Symptoms: The main High-Speed Serial Interface (HSSI) interface flaps when you enter the **map-class frame-relay** global configuration command on a subinterface.

  Conditions: This symptom is observed only when map class contains both traffic shaping and Random Early Detection (RED).

  Workaround: Use only traffic shaping under the map-class.

- CSCeb75485

  Symptoms: No audio may be heard on a Voice over IP (VoIP) call from the public switched telephone network (PSTN) to an H.323 application of a third-party vendor.

  Conditions: This symptom is observed on a Cisco AS5350 that runs Cisco IOS Release 12.2(11)T9. The symptom may also occur in other releases.

  The symptom occurs because no Real-Time Transport Protocol (RTP) stream is created on the Cisco AS5350 when the RTP sequence number is altered by the H.323 application of the third-party vendor during a previous call. Once the RTP sequence number has been altered, all subsequent calls fail.

  Workaround: To enable the Cisco AS5350 to process a single call properly, reboot the Cisco AS5350. However, once the RTP sequence number has been altered, all subsequent calls fail.

- CSCeb75982

  Symptoms: In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment, if you enter the **ping vrf** EXEC command toward the directly connected interfaces of a neighbor's provider edge (PE) router, the ping may fail.

  Conditions: This symptom is observed when aggregate routes on Cisco routers are pinged.

  Workaround: The ping will be successful if you select options when you enter the **ping vrf** EXEC command.

- CSCeb76642

  Symptoms: A Cisco router may reload when you enter the **show ip cef non-recursive detail** EXEC command.

  Conditions: This symptom is observed when any **show** command attempts to display information about tag rewrite entries while the tag rewrite entries are being deleted by route updates.

  Workaround: Do not enter any **show** command to display tag rewrite entries when many route updates occur.

- CSCeb78680

  Symptoms: An Integrated Services Adapter (ISA) may reset and lose its security associations (SAs) or reload unexpectedly.

  Conditions: These symptoms are observed on a Cisco 7200 series that is configured with an ISA when packet memory buffer starvation occurs and when a buffer allocation failure occurs for the Internet Key Exchange (IKE) command path.

  Workaround: Do not use an ISA. Rather, use a Virtual Private Network Acceleration Module (VAM).

  First Alternate Workaround: Reduce the traffic volume.

  Second Alternate Workaround: Remove the bottleneck for the egress packets.

- CSCeb78836

  Symptoms: Cisco IOS software may cause a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message.

Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled:

- **debug h225 asn1**
- **debug h225 events**
- debug h225 q931

Workaround: There is no workaround.

- CSCeb86270

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), the Label Distribution Protocol (LDP) peer address table may become corrupted and cause the router to reload.

  Conditions: This symptom may be observed in situations where three or more routers have advertised the same IP address in LDP address messages. This normally happens when routers have been misconfigured but in very rare circumstances may be done deliberately.

  The circumstance can be recognized by the presence of the following error message:

  ```
  %TAGCON-3-DUP_ADDR_RCVD: Duplicate Address 10.0.0.1 advertised by peer 10.2.2.2:0 is
  already bound to 10.1.1.1:0
  ```

  If only one such message is seen for a given IP address—10.0.0.1 in the above example—then only two routers have advertised the IP address, and only the second is being treated as a duplicate. At least one more such message should be seen if at least three routers have advertised the IP address in question.

  Workaround: The symptom does not occur in typical configurations because duplicate addresses are not configured. If such a configuration is accidentally done, the failure may be avoided if the configuration is corrected before the LDP session to any of the involved peers goes down. If the configuration is deliberate, there is no workaround.

- CSCec02642

  Symptoms: A router may reload with a bus error if a quality of service (QoS) class map or policy map is renamed through modular QoS CLI (MQC) and a subsequent **show memory** EXEC command is issued.

  Conditions: This symptom is observed in all Cisco IOS software releases on all Cisco platforms where the **rename** command is available under class map and policy map modes. It is observed in Cisco IOS Release 12.1 (14)E, Release 12.2(12) and later releases. This symptom is not observed in Release 12.1. The symptom occurs after a global class map or policy map is renamed and a subsequent **show memory** EXEC command is issued.

  Workaround: Avoid use of the **rename** command. Remove and recreate the class map or policy map instead.

- CSCec15517

  Symptoms: A Cisco router may reload when you enter the **show policy-map interface** EXEC command.

  Conditions: This symptom is observed on Cisco 7500 series that is configured with a Frame Relay permanent virtual circuit (PVC) policy.

  Workaround: There is no workaround.

- CSCec15598

  Symptoms: While running Cisco IOS Release 12.2(17a), a Cisco 3640 router may run out of processor memory due to a memory leak in the TCL IVR process.

Conditions: This symptom occurs under the following conditions:

- Only when using Interactive Voice Response (IVR)
- When E1 R2 signaling is configured - When a TCL IVR 1.0 script is used
- Only when DISCONNECT messages arrive with a PI value

Workaround: The memory leak is not present in Cisco IOS Release 12.2(6).

- CSCec15733

  Symptoms: A Cisco router that is running IP over Multiprotocol Label Switching (MPLS) may reload when the Label Distribution Protocol (LDP) responds to the creation of a new session.

  Conditions: This symptom is observed when the router is operating under extremely stressful conditions that cause the CPU utilization to be close to 100 percent. This situation rarely occurs.

  Workaround: There is no workaround.

- CSCec17778

  Symptoms: When you reload a Cisco router, the ATM permanent virtual path (PVP) configuration may disappear and the following error message may be displayed:

  ```
  %ATM: PVP, interface specific setupvp failure
  ```

  Conditions: This symptom is observed on a Cisco 3640 that is configured with an ATM network module but may also occur on another router that is configured with an ATM network module.

  Workaround: Remove the permanent virtual circuit (PVC) configuration, reload the router, and reconfigure the PVP and PVC configuration.

- CSCec18181

  Symptoms: A Cisco 7200 series may reload when you enter the **show pas i82543 interface gigabitEthernet** *interface number* **mta** privileged EXEC command.

  Conditions: This symptom is observed on A Cisco 7200 series that is configured with a Network Processing Engine G-1 (NPE-G1).

  Workaround: There is no workaround.

- CSCec26517

  Symptoms: A Cisco IPSec router with ISDN Dial-on-Demand Routing (DDR) link is unable to bring up a dialer.

  Conditions: This symptom is observed in configurations where the crypto map is applied to dialer interface using the **ip address negotiated** interface configuration command when running Cisco IOS Release 12.2(17a) or Release 12.2(19). This symptom is not observed in Cisco IOS Release 12.2(12) and Release 12.3(1a).

  Workaround: There is no workaround.

- CSCec28505

  Symptoms: When a Cisco router boots up with low-speed serial interface, one error message per interface will show up on the console to disable Cisco IOS legacy fair queue.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCec32135

  Symptoms: **set** commands that are used with a service policy can cause a router to reload in some circumstances. The **set cos** policy-map class configuration command can cause reloads in addition to other set commands.

Conditions: This symptom may be observed with configurations that have a service policy with the set command on the interface in combination with one or all of the following three configurations:

- access-list filtering
- unicast rpf
- multicast routing

Under these circumstances, configuration changes of the **set**-based policy map can cause the router to reload.

Workaround: There is no workaround.

- CSCec34427

  Symptoms: A Cisco router that is running Cisco IOS Release 12.2 (19) or earlier releases may reload following a software-forced reload.

  Conditions: This symptom occurs only on systems that are configured with IP Header Compression (IPHC) and where the amount of free memory is low, or the memory is badly fragmented.

  Prior to the forced reload, the system may log the following error message:

  ```
  %PARSER-2-INTDISABLE: Interrupts disabled in mode interface by command 'ip tcp
  header-compression'
  ```

  Workaround: Ensure that IPHC is disabled, both in the configuration and in any authentication, authorization, and accounting (AAA) (RADIUS) database entries. Use the **no ip tcp header-compression** command and/or the **no ip rtp header- compression** command to disable IPHC.

- CSCec38322

  Symptoms: A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) provider edge (PE) router that is running distributed Cisco Express Forwarding (dCEF) may have high memory usage and memory allocation failures when dCEF is disabled and then reenabled.

  Conditions: This symptom is observed on a PE router that has a large number of VPN routes (over 30,000) in a VPN routing/forwarding (VRF) table when CEF is disabled and then reenabled.

  Further Problem Description: View the output of the **show processes memory** EXEC command to verify that the CEF process memory usage increases.

  Workaround: Reload the router.

- CSCec39685

  Symptoms: Routers that are running Voice over IP (VoIP) are reloading frequently in authentication, authorization, and accounting (AAA) when a combination of an invalid length accounting attribute and too many attributes are being sent to AAA.

  Conditions: This symptom is observed on a Cisco 3660 router that is running Cisco IOS Release 12.2(19). The actual condition which causes VoIP to send an 0 length username is unknown. (CSCec52917 is opened to resolve condition.)

  Workaround: There is no workaround.

- CSCec63438

  Symptoms: The **set** command will not work if used in a non-leaf level in a hierarchical policy.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.3(3).

  Workaround: There is no workaround.

- CSCin41510

  Symptoms: An output service policy with a police feature may be rejected, and the following error message may be generated:

  ```
  Cannot attach flat policy to pvc/sub-interface. Hierarchical policy with shape in
  class-default is recommended
  ```

  Conditions: This symptom is observed when the output service policy is attached to multiple subinterfaces.

  Workaround: There is no workaround.

- CSCin52502

  Symptoms: Ping packets may not pass between a native Gigabit Ethernet port of Cisco 7400 series and a Fast Ethernet port of a Cisco 7500 series.

  Conditions: This symptom is observed when the Cisco 7400 series runs Cisco IOS Release 12.2(18)S.

  Workaround: There is no workaround.

- CSCin56061

  Symptoms: A Cisco router that is running Cisco Gateway GPRS Support Node (GGSN) software shows the count of gsn_used_bandwidth to a bigger value (4294966495) after sending a create PDP context request with different restart counter for an existing PDP.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running the c7200-g5js-mz image.

  Workaround: There is no workaround.

- CSCuk41281

  Symptoms: Traffic forwarding through a traffic engineering (TE) tunnel may not function properly.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2 T.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCeb28654

  Symptoms: If an ISDN physical link is interrupted when dialer backup is implemented using the dialer watch method, a Cisco router may not reestablish the backup connection.

  Conditions: This symptom is observed on a Cisco 2600 series router that is running Cisco IOS Release 12.2(16a).

  Workaround: Set multilink min-link and max-link as 1. This will ensure that there is always one B channel available for dial even when the link toggles and makes the existing call down.

- CSCec39466

  Symptoms: If 40-bit Microsoft Point-to-Point Encryption (MPPE) encryption and Microsoft Point-to-Point Compression (MPPC) are enabled, Cisco IOS will not negotiate just the MPPC with the peer.

  Conditions: This symptom is observed when running Cisco IOS Release 12.2(12h).

  Workaround: There is no workaround.

- CSCec41364

  Symptoms: A Cisco IOS Network Access Server (NAS) may send incorrect port information in accounting records.

  Conditions: This symptom is observed when performing callback without peer authentication.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(19c)

Cisco IOS Release 12.2(19c) is a rebuild release for Cisco IOS Release 12.2(19). The caveats in this section are resolved in Cisco IOS Release 12.2(19c) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCdz32659

  Symptoms: Many memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
  Processor, alignment 0 -Process= "CDP Protocol", ipl= 0, pid= 42 -Traceback= 602D5DF4
  602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
  ```

  Conditions: The symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(17)ST. The symptom may also occur on other Cisco 7500 series routers that run Release 12.0 S, 12.2 S, 12.3, or 12.3 T.

  Workaround: To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCec25430

  Symptoms: A Cisco device reloads on receipt of a corrupt CDP packet. One possible scenario is:

  Reloading a faulty Cisco IP conference station 7935 or 7936 may cause a connected Cisco switch or router to reload. A CDP message may appear on the terminal, such as the following one:

  ```
  %CDP-4-DUPLEX_MISMATCH duplex mismatch discovered on FastEthernet5/1 (not half
  duplex), with SEP00e0752447b2 port 1 (half duplex).
  ```

  Conditions: This symptom is observed when an empty “version” field exists in the output of the **show cdp entry *** command for at least one entry.

  Workaround: Disable CDP by entering the **no cdp run** global configuration command.

  First Alternate Workaround: Disable CDP on the specific (sub-)interface(s) whose corresponding neighbor(s) has or have an empty “version” field in the output of the **show cdp entry *** command.

  Second Alternate Workaround: Disconnect the 7935 or 7936 phone, in the case of the specific symptom that is described above.

- CSCin67568

  Symptoms: A Cisco device experiences a memory leak in the CDP process.

  Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

  Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

Miscellaneous

- CSCdz84583

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain a TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOSÆ software.

  A companion advisory that describes this vulnerability for products that run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml.

- CSCec06146

  Symptoms: A serial interface of a 1-port multichannel E3 port adapter (PA-MC-E3) may fail to enter the “up/up” state when you initially configure the interface or after a number of reconfigurations.

  Conditions: This symptom is observed on a PA-MC-E3 that is installed in a Cisco 7500 series or Cisco 7600 series when the following sequence of events occurs:

  1. You configure an interface by entering the **controller e3** *slot/port* global configuration command followed by the **e1** *line-number* **channel-group** *channel* **timeslots** *range* controller configuration command.

  2. You delete the interface by entering the **controller e3** *slot/port* global configuration command followed by the **no e1** *line-number* **channel-group** *channel* controller configuration command.

  3. You reconfigure the interface by entering the commands listed in Step 1.

  Although the symptom may occur when you initially configure the interface, it is more likely to occur when you configure, delete, and reconfigure the interface several times.

  Workaround: When the interface does not enter the “up/up” state, configure the interface again.

- CSCed35253

  Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

Workaround: Disable IP Inspect and IDS.

- CSCee49862

  Symptoms: A Cisco 7500 series multichannel T3 port adapter (PA-MC-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCin66542

  Symptoms: The line protocol on a T1 of a T3 controller in a PA-MC-2T3+ port adapter may stay in the down state even when looped.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(19b)

Cisco IOS Release 12.2(19b) is a rebuild release for Cisco IOS Release 12.2(19). The caveats in this section are resolved in Cisco IOS Release 12.2(19b) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea19885

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCeb78836

  Symptoms: Cisco IOS software may cause a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message.

  Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled:

  - debug h225 asn1
  - debug h225 events
  - debug h225 q931

  Workaround: There is no workaround.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed28873

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Resolved Caveats—Cisco IOS Release 12.2(19a)

Cisco IOS Release 12.2(19a) is a rebuild release for Cisco IOS Release 12.2(19). The caveats in this section are resolved in Cisco IOS Release 12.2(19a) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCeb73681

  Symptoms: The main High-Speed Serial Interface (HSSI) interface flaps when you enter the **map-class frame-relay** global configuration command on a subinterface.

  Conditions: This symptom is observed only when map class contains both traffic shaping and Random Early Detection (RED).

  Workaround: Use only traffic shaping under the map-class.

- CSCec32135

  Symptoms: "Set" based service-policy can cause the router to reload in some circumstances. The **set cos** command can cause reloads in addition to other **set** commands.

  Conditions: This problem may be seen with configurations that have a service-policy with the **set** command on the interface in combination with one or all of the below three configurations:

  - access-list filtering
  - unicast rpf
  - multicast routing

  Under such circumstances, configuration changes of the "set" based policy-map can cause the router to reload.

  Workaround: There is no workaround.

- CSCin41510

  Symptoms: An output service policy with a police feature may be rejected, and the following error message may be generated:

  ```
  Cannot attach flat policy to pvc/sub-interface. Hierarchical policy with shape in
  class-default is recommended
  ```

  Conditions: This symptom is observed when the output service policy is attached to multiple subinterfaces.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(19)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(19). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(19). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCea30419

  Symptoms: Open Shortest Path First (OSPF) database packets may be exchanged with an invalid length. Error messages may indicate an invalid packet length and bad checksum.

  Conditions: This symptom is observed on a Cisco 7500 series that is running the rsp-js-mz image of Cisco IOS Release 12.2(13)T.

  Workaround: There is no workaround.

- CSCeb20477

  Symptoms: A Cisco router may reload because of a bus error when the **no ip route-cache flow** interface configuration command is enabled on an interface.

  Conditions: This symptom is observed on low-end system platforms that are running Cisco IOS Release 12.2(17) and earlier releases, Release 12.2(14)S, or Release 12.2(10)T and earlier releases.

  Workaround: Do not configure the **ip route-cache flow** interface configuration command on an interface. If the interface is already configured, do not configure the **no ip route-cache flow** interface configuration command.

IBM Connectivity

- CSCdy82170

  Symptoms: The router log indicates that the Bisync interface is going up and down and that the router may reload.

  Conditions: This symptom is observed when Bisync is configured on the serial interface of a Cisco 2600 series router.

  Workaround: There is no workaround.

- CSCea86223

  Symptoms: A router may reload with a segmentation violation (SegV) exception, and the following error message appears:

  ```
  %SYS-3-MGDTIMER
  ```

  Conditions: This symptom is observed on a Cisco 2611 router. The symptom is specific to data-link switching (DLSw) Ethernet redundancy. Any other usage of DLSw does not affect this symptom.

  Workaround: Do not use DLSw Ethernet redundancy. Use DLSw with transparent bridging support. In this case, you can have only one active DLSw router at a time per transparent Ethernet domain.

Interfaces and Bridging

- CSCea38882

  Symptoms: A Cisco 7200 series router may reload because the packet cleanup is not performed completely in the interrupt path of an enhanced ATM port adapter (PA-A3).

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2 and that is configured with a PA-A3 port adapter.

  Workaround: There is no workaround.

- CSCea93100

  Symptoms: Even though a bridge domain is configured, it may not function. A root bridge is placed over the domain that should have been configured. This tree topology problem in the bridge group does not affect any traffic transmission.

  Conditions: This symptom is observed on a Cisco 2600 series router that is running Cisco IOS Release 12.2.

  Workaround: There is no workaround.

- CSCeb04154

  Symptoms: You may see numerous spurious accesses when you configure source-route bridging (SRB) and source-route translational bridging (SRTLB) on the same LAN Emulation (LANE) client.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(6f).

  Workaround: There is no workaround.

- CSCeb60620

  Symptoms: A Cisco 7500 router that is configured as a bridge may not pass bridged traffic on an Ethernet interface. This situation may lead to a loss of connectivity.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running an rsp-jsv-mz image of Cisco IOS Release 12.2(19).

  Workaround: There is no workaround.

- CSCin42584

  Symptoms: A router may not recognize an ATM WAN OC-3 port adapter.

  Conditions: This symptom is observed when an ATM WAN OC-3 port adapter is installed in slot 1 of a Cisco 7200 series router that has a Network Processing Engine 150 (NPE-150).

  Workaround: There is no workaround.

- CSCin43613

  Symptoms: The Fast Ethernet (FE) switching performance on a Cisco 7200 series may be considerably slower than you would expect.

  Conditions: This symptom is observed on any normal FE switching path on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCin46792

  Symptoms: Back-to-back pings with a packet size greater than the configured maximum transmission unit (MTU) may fail.

  Conditions: This symptom is observed on the PA-A2 port adaptor of a Cisco 7200 series router that is running Cisco IOS Release 12.2(16a).

  Workaround: There is no workaround.

IP Routing Protocols

- CSCds24139

  Symptoms: When a source is active, the multicast stream to the receiver may be interrupted for up to 60 seconds.

Conditions: This symptom occurs under the following conditions:

- A redundant router is powered on and takes over the Designated Router (DR) function of the segment.
- The non-DR router wins the assert battle because of a better metric, which causes the DR router to prune its outgoing interface list.

Workaround: There is no workaround.

- CSCea40884

  Symptoms: A Cisco router may reload when you enter the **show ip route vrf** *vrf-name* EXEC command.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(15)T.

  Workaround: There is no workaround.

- CSCea58105

  Symptoms: The interface of a Cisco router that functions as a Protocol Independent Multicast (PIM) rendezvous point may stop receiving traffic. The output of the **show interfaces** privileged EXEC command may show input queue drops.

  Conditions: This symptom is observed after the interface has received PIM register packets with the Router Alert option.

  Workaround: Reload the port adapter or line card with the affected interface.

- CSCea80941

  Symptoms: An Enhanced Interior Gateway Routing Protocol (EIGRP) network fails to query some routes for the second and following topology changes. This results in routing problems.

  Conditions: This symptom is observed in redundant EIGRP networks. The EIGRP neighbor fails to send a query for some routes in the second topology change. The first topology change functions correctly. When the neighbor does not get a reply, the neighbor removes the first route even if the redundant route exists in the network.

  Workaround: Enter the **clear ip eigrp neighbors** EXEC command on all EIGRP routers.

- CSCea81952

  Symptoms: A Network Address Translation (NAT) configuration causes a Cisco router to reload because of H.225 messages.

  Conditions: This symptom is observed on a Cisco router that has the generic transparency descriptor (GTD) enabled by default. The caveat CSCdw86807 committed a GTD feature that has increased the setup TPKT length over the default maximum segment size (MSS) of 536 bytes. This results in TPKT fragmentation, which is not supported by NAT.

  Workaround: Because the GTD feature is enabled by default, disable the GTD feature using the **no isdn gtd** D channel interface configuration command. This removes the TPKT extra length to work with the current NAT restriction of not providing support for application fragmented packets and the default MSS.

- CSCeb12331

  Symptoms: A Cisco router may reload when you simultaneously enter the same command to terminate a router protocol through two different sessions. For example, one session may run via the console and the other session may run via a Virtual Terminal Protocol (VTP). Examples of

commands that terminate a router protocol are the **no router bgp** global configuration command, the **no router isis** global configuration command, the **no router ospf** global configuration command, and so on.

Conditions: This symptom is platform independent.

Workaround: Do not simultaneously enter the same command to terminate a router protocol through two different sessions.

- CSCin36693

  Symptoms: The rendezvous point mapping may not be updated in an existing multicast route state.

  Conditions: This symptom is observed when you change the hash mask length on a bootstrap router (BSR).

  Workaround: There is no workaround. Note that the symptom does not cause any traffic interruption.

ISO CLNS

- CSCeb19730

  Symptoms: A Cisco router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2, Release 12.2 S, Release 12.2 T, Release 12.3 or Release 12.3 T and that is configured with Multiprotocol Label Switching (MPLS) traffic engineering and Intermediate System-to-Intermediate System (IS-IS).

  Workaround: Enter the following command on the router:

  router isis mpls traffic-eng *max-children 0*

Miscellaneous

- CSCds30121

  Symptoms: A Cisco router may stop sending data randomly across any switched virtual circuits (SVCs). This situation is accompanied by "encapsulation error2" failure messages when the **debug atm errors** EXEC command is enabled.

  Conditions: This symptom is observed on a Cisco router with approximately 100 SVCs.

  Workaround: Remove the SVC from the map group, and add it back again.

- CSCdv89200

  Symptoms: A line card may reload.

  Conditions: This symptom is observed when a Turbo access control list (ACL) is removed from a Cisco router while traffic is being processed.

  Workaround: Turn off traffic while making the configuration change.

- CSCdw06558

  Symptoms: A Cisco router may reload if you enter the **no mpls traffic-eng tunnels** command.

  Conditions: This symptom is observed on a Cisco router with about 500 or more tunnels configured.

  Workaround: There is no workaround.

- CSCdx18578

  Symptoms: On a router, the Systems Network Architecture switching services (SNASw) port may transition to an inactive state and all sessions may be lost.

  The router may generate CLSInvalid messages, and SNASw may start to consume memory. If there are sufficient downstream devices, the router may run out of memory and possibly reload.

  Conditions: These symptoms are observed when a SNASw router is using a Hot Standby Router Protocol (HRSP) MAC address for downstream connections, two standby MAC addresses are in use, and a downstream Physical Unit 2.1 (PU2.1) has two link stations, one each to the standby MAC addresses. The symptoms occur when both HSRP MAC addresses are active on the same interface and the downstream device has links active to both MAC addresses.

  Workaround: Move one of the MAC addresses to an internal port, for example to a virtual Token Ring port.

  Alternate Workaround: Configure a second Service Advertising Protocol (SAP) on a second port and configure one of the links of the downstream device to use the second SAP.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdz54555

  Symptoms: An integrated service adaptor (ISA) card resets itself intermittently. The IP Security (IPSec) connections are affected because of the switchover between the hardware crypto engine and the software crypto engine.

  Conditions: This symptom is observed on a Cisco 7200 series router that is configured with an ISA card.

  Workaround: There is no workaround.

- CSCdz55602

  Symptoms: A Cisco router may reload if the **crypto card shutdown/enable** *slot* command is issued with online traffic.

  Conditions: This symptom is observed on a Cisco 7200 series router with a VPN Accelerator Module (VAM).

Workaround: Shut down the input interface before issuing the **crypto card shutdown/enable** *slot* command.

- CSCdz71034

  Symptoms: When "cpmISDNCfgBChannelsInUse" is polled from a network access server (NAS), the total number of active analog and digital calls is returned. The value that is returned does not agree with the results from the **show caller summary** output. It is observed that "cpmISDNCfgBChannelsInUse" returns a value that is one less than the actual value.

  For example: If the total number of calls equals 115 (as verified on the NAS from the **show caller summary** output), polling "cpmISDNCfgBChannelsInUse" returns a value of 114. Similarly, when the total number of calls equals 23, polling "cpmISDNCfgBChannelsInUse" returns a value of 22.

  Conditions: This symptom may be observed on a Cisco AS5400 that is running Cisco IOS Release 12.2(11)T2 and may occur when a large number of both analog and digital calls are received.

  Workaround: There is no workaround.

- CSCdz71219

  Symptoms: The input queue on virtual access interfaces may intermittently fill up and become wedged, causing connections to drop.

  Conditions: This symptom is observed on Cisco AS5300 universal access servers.

  Workaround: There is no workaround.

- CSCdz72292

  Symptoms: After a few weeks of normal operation, the interface on a Cisco PA- MC-8E1 begins flapping and finally pauses with the output queue stuck as follows:

```
Serial1/1:1 is up, line protocol is up
  Encapsulation HDLC, crc 16, Data non-inverted
  Keepalive set (120 sec)
  Last input 00:00:03, output 04:14:23, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 21952
  Queueing strategy: weighted fair
  Output queue: 30/4000/64/21855 (size/max total/threshold/drops)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     43903807 packets input, 3646461183 bytes, 0 no buffer
     Received 0 broadcasts, 321 runts, 0 giants, 0 throttles
     5160 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 2945 abort
     42026998 packets output, 2185017012 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     31 carrier transitions
  no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags
```

  The following traceback is observed in the log:

```
%LINK-4-TOOBIG: Interface Serial60:1, Output packet size of 1526 bytes too big
 Traceback=  0x604007F8  0x604A927C  0x6084E4D4  0x6057425C  0x60CE921C 0x60CE55EC
```

```
%LINK-4-TOOBIG: Interface Serial20:1, Output packet size of 1526 bytes too big
 Traceback=  0x604007F8  0x604A927C  0x6084E4D4  0x6057425C  0x60CE921C 0x60CE55EC
```

Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8E1 interface.

Workaround: There is no workaround.

- CSCdz72673

  Symptoms: A Cisco router that is functioning as a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) provider edge (PE) router may reload with an “address error” message.

  Conditions: This symptom is observed at bootup time when the PE and customer edge (CE) interfaces are coming up. The symptom occurs when a locally learned VPN routing/forwarding (VRF) route temporarily loses its local label. This condition leads to some data structures being cleaned up but still retaining references to the local label. It may also occur after bootup in the case of interface flaps. The reload is not a common occurrence, however, and may need additional triggers.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdv49909. Cisco IOS releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCea01498

  Symptoms: A gateway that negotiates a G.729 codec with 20 bytes in the call setup may send 40 bytes instead.

  Conditions: This symptom is observed on a Cisco AS5300 that is functioning as a gateway.

  Workaround: There is no workaround.

- CSCea19885

  Symptoms: A Cisco router that has a voice feature such as H.323 enabled may reload because of a bus error at address 0xD0D0D0B.

  Conditions: This symptom is observed on a Cisco 3700 series but may also occur on other routers.

  Workaround: There is no workaround.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea35117

  Symptoms: A large number of align-3 spurious error messages may be generated in the log file of a Cisco router.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13a) or Release 12.2(13b).

  Workaround: There is no workaround.

- CSCea35306

  Symptoms: Two Cisco routers that are running Cisco fax relay over a Voice over IP (VoIP) connection may reload after approximately 8 hours of operation.

  Conditions: This symptom is observed in a test using a Cisco 3640 router and a Cisco 3660 router, although the symptom may be platform independent.

  Workaround: There is no workaround.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea42252

  Symptom: The dsx1LineIndex variable for a channelized E1 interface may have an incorrect value for a 1-port multichannel E3 port adaptor (PA-MC-E3).

  Conditions: This symptom is observed when you run the DS1-MIB MIB.

  Workaround: There is no workaround.

- CSCea42620

  Symptoms: A Tag Forwarding Information Base (TFIB) Virtual Private Network version 4 (VPNv4) entry on an Autonomous System Boundary Router (ASBR) for a prefix may not be reinstalled, causing traffic for this prefix to continue to flow to a provider edge (PE) router via the previous best path.

  Conditions: This symptom is observed in a Multiprotocol Label Switching (MPLS) VPN interautonomous system environment in which ASBRs are performing VPNv4 exchanges and in which a Border Gateway Protocol (BGP) session is active.

  The ASBR on which the TFIB VPNv4 entry is not installed should receive a prefix from a Route Reflector (RR) that selects the best of two available paths between the RR and two PE routers. Both PE routers should allocate the same label for the prefix. The PE router to which the best path leads should withdraw the prefix.

  Workaround: Clear the BGP session on the ASBR that is connected to the RR.

  Alternate Workaround: Withdraw the prefix from the ASBR and readvertise the prefix by clearing the prefix on the PE router that advertises the prefix.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea53451

  Symptoms: A Cisco AS5850 may reload after 4 to 5 hours of operation.

  Conditions: This symptom is observed on a Cisco AS5850 that is running Cisco IOS Release 12.2(15)T and that has a call load of 8 calls per second.

  Workaround: There is no workaround.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea55600

  Symptoms: A Frame Relay (FR) interface may go up and down continuously.

  Conditions: This symptom is observed on an FR interface when the keepalive timeout is set to one second and fragmentation and traffic shaping are enabled on multiple permanent virtual circuits (PVCs).

  Workaround: Increase the keepalive timeout to 5 seconds or more.

- CSCea58553

  Symptoms: A Cisco router drops packets in the input queue of the router's interfaces.

```
Router# show interface serial 1/2
Serial1/2 is up,line protocol is up
Hardware is CD2430 in sync mode
Internet address is 10.1.0.1/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
Keepalive not set
LCP Open
Open: IPCP, CCP, CDPCP
Last input 00:00:06, output 00:00:37, output hang 2d00h
```

```
Last clearing of "show interface" counters 1d20h
Input queue: 0/75/9847/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
891420 packets input, 62654151 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
890285 packets output, 1175436268 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets 0 output buffer failures,
0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Conditions: This symptom is observed on a Cisco router that uses hardware compression. The packet drops occur sporadically when there are no errors reported on the interface and CPU utilization is below 10 percent. The pace at which the packets are dropped accelerates over time and affects more and more traffic.

Workaround: There is no workaround.

- CSCea64842

  Symptoms: A Cisco router that is used to fast-switch fragmented Multilink PPP (MLP) packets may corrupt the packets. The output from the **debug ip error** EXEC command shows the following error:

  ```
  IP: s=10.254.254.25 (Multilink1), d=10.254.34.2, len 100, d ispose icmp.checksumerr
  ```

  A packet dump indicates that part of the MLP header has been inserted in the packet payload:

  ```
  IP: s=10.254.254.25 (Multilink1), d=10.254.34.2 (Multilink1 ), len 100, rcvd 3
  03845B50: FF030021 45000064 004A0000 ...!E..d.J.. 03845B60: FD018737 0AFEFE19
  0AFE2202 00005804 }..7.~~..~"...X. 03845B70: 1EB81580 00000000 0159F8B4
  ABCDABCD .8.......Yx4+M+M 03845B80: ABCDABCD ABCDABCD ABCDABCD ABCDABCD
  +M+M+M+M+M+M+M+M 03845B90: ABCDABCD ABCDFF03 003D4000 1939ABCD
  +M+M+M...=@..9+M 03845BA0: ABCDABCD ABCDABCD ABCDABCD ABCDABCD
  +M+M+M+M+M+M+M+M 03845BB0: ABCDABCD ABCDABCD ABCDABCD 00 +M+M+M+M+M+M.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured with fast switching. The symptom is not observed if the process switching path is used or if the packet is too small to fragment.

  Workaround: There is no workaround.

- CSCea69733

  Symptoms: The selective packet discard (SPD) feature does not function correctly on the E0 interface of a Cisco AS5300 router.

  Conditions: This symptom is observed on a Cisco AS5300 router.

  Workaround: Increase the input hold queue.

- CSCea70448

  Symptoms: A DistributedDirector may reload when the **clear ip dir servers** EXEC command is entered.

Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(11).

Workaround: There is no workaround.

- CSCea70473

  Symptoms: A memory leak may occur in the PPP authorization process on a Cisco 7206VXR.

  Conditions: This symptom is observed on a Cisco 7206VXR that is running Cisco IOS Release 12.2(16) and that is configured for PPP over Ethernet (PPPoE). The symptom may occur on any Cisco router that is running Cisco IOS Release 12.2(16).

  Workaround: There is no workaround.

- CSCea72272

  Symptoms: The startup configuration file may become corrupt.

  Conditions: This symptom is observed when multiple Telnet sessions simultaneously execute the **copy running-config startup-config** EXEC command. Only one Telnet session at a time should execute the **copy running-config startup-config** EXEC command.

  Workaround: To save the configuration properly, reenter the **copy running-config startup-config** EXEC command.

- CSCea75286

  Symptoms: A Cisco router may reload because of a bus error at address 0x3.

  Conditions: This symptom is observed on a Cisco 3660 router that has an Advanced Integration Modules-Virtual Private Network (AIM-VPN), an IP Security (IPSec) configuration, and that is running Cisco IOS Release 12.1(5)T10 or Release 12.2(16).

  Workaround: There is no workaround.

- CSCea75663

  Symptoms: A router that is configured with Network Address Translation (NAT) does not behave correctly if outside source static is configured but no inside source static is configured. The symptom is not observed if there is at least one inside source static configured in addition to the outside source static.

  Conditions: This symptom is observed on a router that is configured with NAT and is observed with Internet Control Message Protocol (ICMP) messages type 3 code 4 (ICMP unreachables with the DF bit set). A possibly related caveat is CSCds82679.

  Workaround: There is no workaround.

- CSCea77328

  Symptoms: A Cisco uBR905 incorrectly sources a Dynamic Host Configuration Protocol (DHCP) request packet from a cable modem interface.

  Conditions: This symptom is observed during the DHCP proxy process.

  Workaround: There is no workaround.

- CSCea78007

  Symptoms: REQACTPU is rejected with an 08060000 sense code. SNA Switching Services (SNASw) may not stop the link station so that the end device can try another data-link switching (DLSw) peer. The SNASw link and the DLSw TCP/IP circuit stay intact so the physical unit (PU) continues to retry on an invalid host, which affects sites that peer to multiple hosts.

  Conditions: This symptom is observed in Cisco IOS Release 12.1(15) or Release 12.2(12) and later releases. A design change was introduced via CSCdw93088 to cause the circuit not to break.

Workaround: Manually break the circuit so that DLSw can use the other DLSw peer.

- CSCea81256

  Symptoms: The Transparent Common Channel Signaling (T-CCS) frame forwarding connection does not work correctly on a Cisco router that is configured with a digital voice port adapter (PA).

  Conditions: This symptom is observed when one router has a VXC-2TE1+ digital voice PA and the other router has a PA-MCX-RTE1 digital voice PA, and the routers are running Cisco IOS Release 12.2(a) or later releases.

  Workaround: Run Cisco IOS Release 12.2 T on the router with the PA-MCX card.

- CSCea81777

  Symptoms: Calls that originate from a public switched telephone network (PSTN) with E1 R2 protocol and go to channel-associated signaling (CAS) doing hairpin may not work.

  Conditions: This symptom is observed with a PBX that is connected to a Cisco router with a CAS interface. The CAS interface works well with all remote sites. The router then connects to a PSTN by way of E1 R2. The calls work well from the PBX to the PSTN. Incoming calls from the PSTN ring the phone in the PBX once, and then the calls are dropped.

  Workaround: There is no workaround.

- CSCea82183

  Symptoms: The following error message is displayed on an Automated Teller Machine (ATM) when it is powered down:

  ```
  %BSC-3-BADLINESTATE
  ```

  Conditions: This symptom is observed on a Cisco router that has the following configuration:

  - A Cisco 2600 router is configured with a 1-port serial WAN interface card (WIC- 1T), and acts as a data terminal equipment (DTE) router and is running Cisco IOS Release 12.2(10a).
  - A router is connected to one ATM machine as a Binary Synchronous Communications (BSC) Block Serial Tunnel (BSTUN).

  When the ATM is powered down, the "%BSC-3-BADLINESTATE" error message is displayed and then the ATM is powered back up. The BSC/BSTUN router does not start to send any frames, even sporadically.

  The output from the **show bsc** EXEC command displays the message "Out of SYN-hunt mode." The output from the **show interfaces serial** EXEC command of the BSTUN encapsulations never displays increments of the output packet count.

  Workaround: There is no workaround.

- CSCea84736

  Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface, pings may fail on this interface.

  Conditions: This symptom is observed on an interface that has both PPP and Intermediate System-to-Intermediate System (IS-IS) configured.

  Workaround: There is no workaround.

- CSCea84911

  Symptoms: A slow-start call may fail because a Cisco universal gateway that is functioning as an H.323 gateway may not send an Open Logical Channel (OLC) message, causing the call to time out.

  Conditions: This symptom is observed in approximately one out of every 200 calls when the originating endpoint is a slow-start endpoint, such as Cisco CallManager.

Workaround: If possible, configure fast start on the originating endpoint. (In a fast-start configuration, no OLC messages are sent.)

- CSCea85410

  Symptoms: A Cisco router may reload when interactive voice response (IVR) calls are involved.

  Conditions: This symptom is observed on a Cisco AS5300 router.

  Workaround: There is no workaround.

- CSCea86857

  Symptoms: A Cisco IOS Domain Name System (DNS) server may drop DNS queries from clients. The following error message may be logged:

  ```
  %DNSSERVER-3-UDPDNSOVERLOAD: Excessive DNS query overloading:
  dropping <packet-id> from <client-address >
  ```

  Conditions: This symptom occurs if the CPU load for the router is high when DNS queries come in.

  Workaround: There is no workaround.

- CSCea89362

  Symptoms: Spurious accesses may be recorded on a Cisco 7206VXR router with a network services engine 1 (NSE-1) processor.

  Conditions: This symptom is observed on a Cisco 7206VXR router with a NSE-1 processor that is running Cisco IOS Release 12.2(17).

  Workaround: Turn off the Parallel eXpress Forwarding (PXF) processor by enabling the **no ip pxf** global command.

- CSCea90394

  Symptoms: A customer of a service provider (SP) may report poor performance across new long-distance (over 100 km) E3 lines with a file transfer rate of about 3 to 5 Mbps. Frame check sequence (FCS) errors may occur in G.751 frames, “Time to Live,” “Transport Retransmission,” and “TCP Connection Reset by Server” conditions, and other conditions may occur in the LAN. The symptoms are caused by difficulties with the clock signal.

  Conditions: These symptoms are observed on a Cisco 7200 series, Cisco 7500 series, and Cisco 7600 series that are configured with a 1-port E3 serial port adapter (PA-E3), but these symptoms may also occur on a 2-port E3 serial port adapter (PA-2E3). The symptoms are not platform specific but port-adapter specific. The symptoms are not observed when short-distance E3 lines are used.

  The clocking is not provided by the Plesichronous Digital Hierarchy (PDH)/Synchronous Digital Hierarchy (SDH) network of the SP but by the internal clock source of one of the routers of the SP customer (that is, the **clock source internal** controller configuration command is configured), while another router of the SP customer is configured as the clock slave (that is, the **clock source line** controller configuration command is configured). However, the symptom may also occur when the clocking is provided by the SP.

  When a line interruption occurs, the PA-E3 on which the **clock source line** controller configuration command is configured may not switch back its transmitter clock (which should be synchronized from the incoming clock signal of the line) from internal clocking to line clocking. When the line is down, the router in which this PA-E3 is installed temporarily uses its internal clock signal. When the line comes back up again, the router should switch back to the line clock signal.

  Long-distance lines are affected because the router that receives traffic over long-distance lines requires a relatively long time to synchronize its clock via line clock signal. The symptoms are observed during the initial link up and during line interruptions.

Workaround: Use enhanced 1-port ATM E3 port adapters (PA-A3-E3) on which the clocking difficulties do not occur.

Temporary Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the serial interface of the affected PA-E3. Doing so provides a workaround until the next line interruption.

- CSCea93882

  Symptoms: If Cisco Express Forwarding (CEF) is disabled, a router may reload with the following error message upon the receipt of a malformed generic routing encapsulation (GRE) packet:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0xA30, pc=0x40992D3C,
  ra=0x405E64B8, sp=0x43562838
  ```

  Conditions: This symptom is observed on a Cisco router that has CEF disabled. The symptom even occurs without a tunnel configuration on the router.

  Workaround: Enable CEF on the router by entering the **ip cef** global configuration command.

- CSCea94063

  Symptoms: A Cisco voice gateway that is configured for H.323 and Fast Start may not correctly negotiate the codec payload size upon a call transfer when the codec of the initial call is different from the codec for the transferred call.

  The following additional symptoms may be observed:

  – There is no audio from the H.323 gateway to the IP phones after the call transfer.

  – From the Call Statistics screen on the IP phone, IP phone B reports the RxSize to be 0 ms and RxDisc rapidly increments.

  Conditions: These symptoms are observed on a Cisco voice gateway that is running Cisco IOS Release 12.2(8)T5 and that has Cisco CallManager configured to receive H.323 Fast Start calls. These symptoms may not be limited to this configuration and may be observed in other environments as well.

  The public switched telephone network (PSTN) caller's initial call to IP phone A uses G.711 ulaw as the codec, but the transferred call to IP phone B is configured for G.729.

  Workaround: Disable Fast Start on the Cisco CallManager.

  Alternate Workaround: Configure all calls for the same codec.

- CSCeb00104

  Symptoms: When configuration changes are made, a Cisco 7500 series Versatile Interface Processor (VIP) may pause indefinitely, produce large numbers of spurious memory accesses, or reload. This situation may cause the router to detect that interfaces on the VIP are not sending packets and to report that the output of the interfaces is stuck.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for fragmentation and shaping on a Frame Relay interface using modular QoS CLI (MQC).

  Workaround: Before you make quality of service (QoS) policy or Frame Relay fragmentation changes on an interface of the VIP, enter the shutdown interface configuration command on the interface.

- CSCeb02068

  Symptoms: In a configuration with multiple name servers, when one server times out, the other servers may not be contacted during name resolution.

  Conditions: This symptom is observed when the **ip domain- list** *name* global configuration command is enabled.

Workaround: Replace the **ip domain-list** *name* global configuration command with the **ip domain-name** *name* global configuration command.

Alternate Workaround: Explicitly specify a domain when resolving a name. For example, enter "anyname.cisco.com" instead of "anyname."

- CSCeb04441

  Symptoms: When an ATM link flaps or a remote ATM platform reloads, a Fast Etherchannel may fail and Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors that are connected via the Fast Etherchannel may be lost.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-pv-mz image of Cisco IOS Release 12.0(21)S5.

  Workaround: There is no workaround.

- CSCeb05519

  Symptoms: The core router Multiprotocol Label Switching (MPLS) forwarding entry has the correct outgoing interface but has an incorrect label to use for sending traffic to the edge router. The incorrect label is identical to the label that is sent by another core router for the same prefix through another interface.

  Conditions: This symptom is observed in a service provider network when the route to the prefix that has the incorrect MPLS forwarding entry is configured using a static recursive route and the specific IP address that is specified in the **ip route** *prefix mask ip-address* global configuration command is changed by topology changes to go through a different adjacent router. The incorrect outgoing Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP) label corresponds to the router that was adjacent prior to the routing change.

  Workaround: To clear this condition, enter the **clear ip route** {*network* [*mask*] | *} EXEC command to cause MPLS to create a new forwarding entry that has the correct interface and label for the prefix.

  To prevent this condition from occurring, advertise the route to the prefix in question using an Interior Gateway Protocol (IGP).

  Alternate Workaround: Configure a static nonrecursive route to the prefix and IP address of the next-hop router by entering the **ip route** *prefix mask ip-address interface-type interface-number* global configuration command.

- CSCeb05672

  Symptoms: Cisco IOS Server Load Balancing (SLB) packets that are switched at the process level instead of at the Forwarding Information Base (FIB) level may be dropped by a Cisco router.

  Conditions: This symptom is observed when the virtual IP destination address is a dynamic alias, which occurs when the virtual IP destination address is a member of a subnet on the interface of a router.

  Workaround: Enable Cisco Express Forwarding (CEF) switching by entering the **ip cef** global configuration command, and enter the **ip route-cache cef** interface configuration command on the destination interface.

- CSCeb06567

  Symptoms: The NetFlow microcode may be flawed and cause the Parallel Express Forwarding (PXF) engine to reload with the following error message:

  IHB Exception - watchdog timer expired

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Service Engine (NSE) and on a Cisco 7401.

  Workaround: Disable PXF if this is an option. Otherwise, there is no workaround.

- CSCeb06842

  Symptoms: A Cisco MC3810 multiservice access concentrator may reload by either a software-forced reload or an address error.

  Conditions: This symptom occurs when the router is running either Cisco IOS Release 12.2(7c) or Release 12.2(16a).

  Workaround: There is no workaround.

- CSCeb09287

  Symptoms: It may be difficult to make an Inverse Multiplexing over ATM (IMA) link between a Cisco router and other vendor equipment.

  Conditions: This symptom is observed on Cisco 2600 series and Cisco 3600 series routers. When an IMA link is configured between the Cisco 2600 series and the Cisco 3600 series and other vendor equipment, the Cisco routers keep sending the **test link** command (set to 1) in the IMA Control Protocol (ICP) cell regardless of the **ima test** interface configuration command. Both the Cisco 2600 series and Cisco 3600 series platforms need the fix for the caveat CSCds55768 to eliminate this symptom.

  Workaround: There is no workaround.

- CSCeb13026

  Symptoms: The Cisco IOS TACACS+ is not able to communicate with a TACACS+ server.

  Conditions: This symptom occurs when no authentication and encryption key has been configured.

  Workaround: Define a key.

- CSCeb14562

  Symptoms: A Gigabit interface bounces when a bridge group is either added or removed from the Gigabit subinterface. Traffic stops on all other subinterfaces until the interface comes back up again.

  See the following example:

```
interface GigabitEthernet0/1
 no ip address
 duplex full
 speed 1000
 media-type gbic
 no negotiation auto
!
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
!
interface GigabitEthernet0/1.11
 encapsulation dot1Q 11
 bridge-group 11
!
interface GigabitEthernet0/1.12
 encapsulation dot1Q 12
 bridge-group 12
NPE-G1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
NPE-G1(config)# interface GigabitEthernet0/1.10
NPE-G1(config-subif)# bri
NPE-G1(config-subif)# bridge-group 10
NPE-G1(config-subif)#
```

At this point the corresponding switchport shows the following:

```
2003 May 19 18:19:18 %ETHC-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
2003 May 19 18:19:18 %DTP-5-NONTRUNKPORTON:Port 1/1 has become non-trunk
2003 May 19 18:19:59 %DTP-5-TRUNKPORTON:Port 1/1 has become dot1q trunk
2003 May 19 18:20:12 %ETHC-5-PORTTOSTP:Port 1/1 joined bridge port 1/1Conditions:
```

Conditions: This symptom is observed on a Cisco 7200 series Network Processing Engine G1 (NPE-G1).

Workaround: There is no workaround. Use the **set spantree portfast** *mod_num/port_num* **enable** command in privileged mode to configure "spanning tree PortFast" on a trunk on the switchport to reduce the duration of the outage.

- CSCeb27452

  Symptoms: A Cisco router that functions in a Multiprotocol Label Switching (MPLS) environment may reload unexpectedly with a bus error.

  Conditions: This symptom is observed under rare circumstances when the router attempts to send an Internet Control Message Protocol (ICMP) packet that was triggered by an MPLS packet.

  Workaround: There is no workaround.

- CSCeb29070

  Symptoms: When you enter the **copy running-config startup-config** EXEC command or any other configuration mode command, the copy process may not be successful or the configuration may not be saved, and a "File table overflow" error message may be generated.

  Conditions: This symptom is observed on a Cisco router that is configured with dual Route Processors (RPs) and that runs Cisco IOS Release 12.0(23)S2 when you enter any configuration command while the **show running-config** EXEC command is being executed, which takes a relatively long time when the running configuration has a large size.

  Workaround: Do not enter any configuration command while the **show running-config** EXEC command is being executed.

- CSCeb34203

  Symptoms: A Cisco router may experience output queue packet drops on the priority queue before the interface is congested on an E1 serial interface on a PA-MC-E3.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.1(18)E.

  Workaround: Use the **tx-ring-limit** interface configuration command to increase the value of the drivers transmitted on the queue. Refer to the following document for additional information:

  http://www.cisco.com/warp/customer/121/txringlimit_6142.html

- CSCeb34375

  Symptoms: A Cisco router may drop packets that are received from the peer router if the packets are doing Protocol Field Compression.

Conditions: This symptom is observed on a Cisco 7500 series router that is running Multilink PPP (MLP) with distributed Cisco Express Forwarding (dCEF) enabled. This symptom is not seen with Route Switch Processor (RSP) based CEF.

Workaround: Reset the multilink interface.

- CSCeb35210

  Symptoms: A router that is running Cisco IOS Release 12.2 may display alignment errors or exhibit a bus error reload during normal mode of operation.

  Conditions: This symptom is observed on a Cisco router that is configured for quality of service (QoS).

  Workaround: Remove the QoS configuration.

- CSCeb37410

  Symptoms: The name of an interface in the output of the **show ip vrf interfaces** EXEC command may be truncated to 22 characters.

  Conditions: This symptom is observed on a provider edge (PE) router that has Virtual Private Network (VPN) routing/forwarding (VRF) configured on an interface when the name of the interface is longer than 22 characters.

  Workaround: To display the full name of the interface, enter the **show ip vrf** EXEC command, that is, without the **interfaces** keyword.

- CSCeb38896

  Symptoms: When a Cisco router tries to produce a RADIUS packet, the following error message is produced:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  The error message is followed by a traceback and is produced even if the packet contains only a small number of attributes that are not large enough to overflow the temporary buffer used to construct the packet.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2.

  Workaround: There is no workaround.

- CSCeb43378

  Symptoms: A Cisco router may have a software-forced reload when the **show interfaces virtual-access** *number* [**configuration**] EXEC command is entered.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(17).

  Workaround: Do not use the **show interfaces virtual-access** *number* [**configuration**] EXEC command.

- CSCeb45208

  Symptoms: An integrated service adaptor (ISA) card may cease to process commands and packets, which results in a crypto-processing deadlock. An error "1510" will typically result, and packet flow through the card will cease.

  Conditions: This symptom is observed on a Cisco 7200 series router that is using Cisco Express Forwarding (CEF) or fast switching. The router is using an ISA card and is configured such that a single packet requires multiple passes through the ISA (such as a hub router terminating multiple tunnels and/or using generic routing encapsulation [GRE] with IP Security [IPSec]). Under these conditions a burst of traffic, or generally medium-to-high traffic levels (above 40Mbps), may trigger the symptom.

Workarounds:

- Use a VPN Acceleration Module (VAM) in place of an ISA as a viable alternative.
- Use process switching.

- CSCeb49581

  Symptoms: A linkUp trap may not be generated on a Cisco router.

  Conditions: This symptom is observed on a Cisco 3620 router that is running Cisco IOS Release 12.2(17).

  Workaround: There is no workaround.

- CSCeb49678

  Symptoms: A Cisco 3620 router may experience a software-forced reload when constant bit rate (CBR) is configured.

  Conditions: This symptom is observed on a Cisco 3600 series router that is running Cisco IOS Release 12.2(17).

  Workaround: Shut down the interface or subinterface before modifying the configuration.

- CSCeb53422

  Symptoms: The call fallback subsystem hard-codes the amount of time it will wait for the response to the probes to 300 milliseconds. The probes fail if the round-trip time is more than 300 milliseconds, even though the network is high bandwidth. The timer to wait for the probes should be configurable for high delay links. This will result in call setup failure.

  Conditions: This symptom is observed on platforms that are running Cisco IOS Release 12.2(16). The symptom happens for high delay links (with a round-trip time greater than 300 milliseconds).

  Workaround: There is no workaround.

- CSCeb68061

  Symptoms: In an interautonomous setup in the Autonomous System Boundary Router (ASBR), the label for a prefix in the label forwarding information base (LFIB) may be inconsistent with the actual label in the multiprotocol external Border Gateway Protocol (MP-eBGP) table.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 12.2.

  Workaround: Execute the **clear ip bgp** *neighbor-address* privileged EXEC command where *neighbor-address* is the address of the eBGP peer from which we learn the route to the prefix whose label is wrong.

- CSCeb78836

  Symptoms: Cisco IOS software may cause a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message.

  Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled:

  - debug h225 asn1
  - debug h225 events
  - debug h225 q931

  Workaround: There is no workaround.

- CSCin28487

  Symptoms: When a channel group is deleted and recreated on an 8-port multichannel T1/E1 8PRI port adapter (PA-MC-8TE1+), error messages and tracebacks may be generated. No functionality is affected because of these tracebacks.

  Conditions: These symptoms are observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2 S.

  Workaround: There is no workaround.

- CSCin39148

  Symptoms: A line card may reload when header compression is disabled.

  Conditions: This symptom occurs when header compression is disabled when the **show ip rtp header-compression** command is executed from another window and is waiting on "more."

  Workaround: Do not disable header compression in the middle of enabling the **show ip rtp header-compression** command.

- CSCin39446

  Symptoms: Traffic may pause indefinitely on a few channels of certain port adapters.

  Conditions: This symptom is observed on the following port adapters:

  - PA-MC-xT1
  - PA-MC-xE1
  - PA-MC-xT3
  - PA-MCX-xTE1

  Workaround: Reprovision the affected channels on the port adapters.

- CSCin41495

  Symptoms: After digital signal processors (DSPs) are configured on a Cisco router, the corresponding controllers cannot be located. The command-line interface (CLI) does not allow the correct controllers to be selected.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with DSPs.

  Workaround: There is no workaround.

- CSCin43828

  Symptoms: A traceback and register display with a cause is listed as follows:

  ```
  Cause 0000041C (Code 0x7): Data Bus Error exception
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(17). The condition reported was associated with a router that was being operated outside of its temperature parameters. Other physical or hardware associated issues could lead to this condition.

  Workaround: There is no workaround.

- CSCin46471

  Symptoms: Time division multiplexing (TDM) hairpinned calls are using digital signal processor (DSP) resources. The TDM hairpinned call should not continue using DSP resources and will release the resources once the call gets hairpinned.

  Conditions: This symptom is observed on a Cisco AS5350 universal gateway.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCdz42788

  Symptoms: When you make ISDN configuration changes on a Cisco 7204VXR router, bus errors may occur.

  Conditions: This symptom is observed on a Cisco 7204VXR router that is running Cisco IOS Release 12.2(12a).

  Workaround: There is no workaround.

- CSCea19800

  Symptoms: When a user connects to an access control list (ACL) that is applied inbound on a virtual template, the ACL fails to deny traffic if the **deny ip any any** router configuration command has been configured and fails to register a match (hit counts) on the ACL.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(11)T3 or Release 12.2(13)T1. The symptom occurs with inbound ACLs not with outbound ACLs.

  Workaround: There is no workaround.

- CSCea21643

  Symptoms: The dialer watch may stall, and a Cisco router may pause permanently.

  Conditions: This symptom is observed when an ISDN link flaps.

  Workaround: There is no workaround.

- CSCea48995

  Symptom: The information element (IE) of a calling party number in an outgoing call setup message may be corrupted. When you use the Q.931 Translator, the log files may display that the calling party number in the outgoing call setup message is "0x00," as in the following example:

  ```
  ISDN Se0:23: TX -> SETUP pd = 8 callref = 0x0005 Bearer Capability i = 0x8890 Channel
  ID i = 0xA98397 Calling Party Number i = 0x00, (null), Plan:Unknown, Type:Unknown
  Calling Party SubAddr i = 0x80, '9876' Called Party Number i = 0x80, '2222',
  Plan:Unknown, Type:Unknown
  ```

  Condition: This symptom is observed after an IE for a calling party subaddress is received.

  Workaround: There is no workaround.

- CSCea51222

  Symptoms: Rare X.25 reset events and an "X.25 Data packet, Bad P(S), Receive window violation" error message may occur on a router. The "P(S)" value, however, is in sequence and within the receive window.

  Conditions: This symptom is observed under rare circumstances when there is a heavy X.25 transmit load on the router.

  Workaround: There is no workaround.

- CSCea51540

  Symptoms: The IP Control Protocol (IPCP) times out on a link control protocol (LCP) negotiation.

  Conditions: This symptom is observed when dial-up networking (DUN) is used to connect to a Cisco router. Subsequent calls will fail in LCP. The symptom is not observed if the user is using only PPP.

  Workaround: There is no workaround if both dialing methods are requested.

- CSCea70357

  Symptoms: Frame Relay traffic shaping may become inactive.

  Conditions: This symptom is observed when the IP maximum transmission unit (MTU) is changed on a serial subinterface that is configured for Frame Relay and traffic shaping.

  Workaround: There is no workaround.

- CSCea76050

  Symptoms: An IP phone does not display the calling party name for an inbound call through an H.323 gateway that uses a primary Digital Multiplex System (DMS-100).

  Conditions: This symptom is observed when a call is sent to a router on an ISDN primary DMS-100 trunk where the “displayIE” does not start with the special leading character required by the DMS specification. The call flow is from Plain Old Telephone Service (POTS) to Voice over IP (VoIP).

  Workaround: Use Cisco IOS Release 12.2(10a) or any Cisco IOS release without the fix for CSCdx12421. CSCdz86750 addresses this issue in the VoIP-to-POTS direction.

- CSCea87639

  Symptoms: A Cisco 7200 series router may occasionally send START-CONTROL-REPLY control messages with the reserved field set to a value other than zero.

  Conditions: This symptom is observed on a Cisco 7200 series router that is setting up Point-to-Point Tunneling Protocol (PPTP) tunnels.

  Workaround: There is no workaround.

- CSCea90880

  Symptoms: When you enter the **show frame-relay pvc** privileged EXEC command, a Cisco router may reload because of a bus error.

  Conditions: This symptom is observed when two users simultaneously edit the same data-link connection identifier (DLCI).

  Workaround: Ensure that only one person at a time edits a DLCI.

- CSCeb18111

  Symptoms: A Layer 2 Tunneling Protocol (L2TP) session may flap intermittently because of wedged interfaces.

  Conditions: This symptom is observed on a Cisco 7500 series after a few days of proper operation. With the exception of the Cisco 3600 series, Cisco 7200 series, and Cisco 7400 series, the symptom may also occur on other platforms.

  Workaround: Reload the router.

- CSCeb39295

  Symptoms: When the **backup interface dialer** *number* interface configuration command is enabled under the primary serial interface, the dialer interfaces may not initiate outgoing calls through ISDN BRI lines if the line protocol status was switched from standby to up.

  Conditions: This symptom is observed on a Cisco 7200 series router.

  Workaround: Shut down the dialer interface that cannot trigger the outgoing call and create new dialer interfaces.

- CSCin43573

  Symptoms: The IP Control Protocol (IPCP) may fail when a Multilink PPP (MLP) link attempts to reestablish itself after it is terminated.

Conditions: This symptom is observed when an MLP link attempts to reestablish itself after it is terminated on a Cisco 827.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(17f)

Cisco IOS Release 12.2(17f) is a rebuild release for Cisco IOS Release 12.2(17). The caveats in this section are resolved in Cisco IOS Release 12.2(17f) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.
- CSCei76358

  Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

Resolved Caveats—Cisco IOS Release 12.2(17e)

Cisco IOS Release 12.2(17e) is a rebuild release for Cisco IOS Release 12.2(17). The caveats in this section are resolved in Cisco IOS Release 12.2(17e) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext

Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally.

Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

Workaround: The detail advisory is available at
http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

IP Routing Protocols

- CSCee67450

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  Cisco has made free software available to address this problem.

  This issue is tracked by CERT/CC VU#689326.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages

  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:
  http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Miscellaneous

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

- CSCef44225

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages

  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages

  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

Resolved Caveats—Cisco IOS Release 12.2(17d)

Cisco IOS Release 12.2(17d) is a rebuild release for Cisco IOS Release 12.2(17). The caveats in this section are resolved in Cisco IOS Release 12.2(17d) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCed28873

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

Miscellaneous

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Resolved Caveats—Cisco IOS Release 12.2(17b)

Cisco IOS Release 12.2(17b) is a rebuild release for Cisco IOS Release 12.2(17). The caveats in this section are resolved in Cisco IOS Release 12.2(17b) but may be open in previous Cisco IOS releases.

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.

- CSCea80820

  Symptoms: A Cisco router with ATM interface(s) with Address Resolution Protocol (ARP) enabled may experience alignment corrections as shown below:

  ```
  %ALIGN-3-CORRECT: Alignment correction made
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router but is not platform dependent.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(17a)

Cisco IOS Release 12.2(17a) is a rebuild release for Cisco IOS Release 12.2(17). The caveats in this section are resolved in Cisco IOS Release 12.2(17a) but may be open in previous Cisco IOS releases.

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.

Interfaces and Bridging

- CSCea38882

  Symptoms: A Cisco 7200 series router may reload because the packet cleanup is not performed completely in the interrupt path of an enhanced ATM port adapter (PA-A3).

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2 and that is configured with a PA-A3 port adapter.

  Workaround: There is no workaround.

- CSCin42584

  Symptoms: A router may not recognize an ATM WAN OC-3 port adapter.

  Conditions: This symptom is observed when an ATM WAN OC-3 port adapter is installed in slot 1 of a Cisco 7200 series router that has a Network Processing Engine 150 (NPE-150).

  Workaround: There is no workaround.

- CSCin43613

  Symptoms: The Fast Ethernet (FE) switching performance on a Cisco 7200 series may be considerably slower than you would expect.

  Conditions: This symptom is observed on any normal FE switching path on a Cisco 7200 series.

  Workaround: There is no workaround.

Miscellaneous

- CSCdz54555

  Symptoms: An integrated service adaptor (ISA) card resets itself intermittently. The IP Security (IPSec) connections are affected because of the switchover between the hardware crypto engine and the software crypto engine.

  Conditions: This symptom is observed on a Cisco 7200 series router that is configured with an ISA card.

  Workaround: There is no workaround.

- CSCea35117

  Symptoms: A large number of align-3 spurious error messages may be generated in the log file of a Cisco router.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13a) or Release 12.2(13b).

  Workaround: There is no workaround.

- CSCeb06567

  Symptoms: The NetFlow microcode may be flawed and cause the Parallel Express Forwarding (PXF) engine to reload with the following error message:

  ```
  IHB Exception - watchdog timer expired
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Service Engine (NSE) and on a Cisco 7401.

  Workaround: Disable PXF if this is an option. Otherwise, there is no workaround.

Wide-Area Networking

- CSCea21643

  Symptoms: The dialer watch may stall, and a Cisco router may pause permanently.

  Conditions: This symptom is observed when an ISDN link flaps.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(17)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(17). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(17). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCdu07504

  Symptoms: A Cisco router may reload because of a software condition when you enter the **show voice dsp** EXEC command. The following message is displayed when you enter **the show version** EXEC command:

  ```
  <router name> uptime is 10 minutes
  System returned to ROM by error - software forced crash, PC 0x2242AC
  System image file is <file name>
  ```

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(5)XM2 but may also occur in other releases such as Release 12.2 T.

  Workaround: There is no workaround.

- CSCdx04081

  Symptoms: A Cisco MC3810 router with a T1 controller may report line code violation (LCV) errors.

  Conditions: This symptom is observed on a Cisco MC3810 router with a T1 controller.

Workaround: There is no workaround. The LCV errors are false errors and do not have an impact on the performance of the router. This symptom may be verified by using the **show controllers t1** EXEC command.

- CSCdx07849

  Symptoms: An attempt to update the startup-config file using the **write memory** EXEC command may fail with the following error:

  ```
  startup-config file open failed (Device or resource busy)
  ```

  Conditions: This symptom may be caused by a process that is attempting to update NVRAM. To locate this process, use the **show file descriptors** EXEC command:

  ```
  Router# show file descriptors
  File Descriptors: FD Position Open PID Path 0 0 430A 157 nvram:
  ```

  Use the **show processes** EXEC command to find the process with the offending physical identification (PID). If the PID belongs to a process called “radius nvwrite,” this caveat may cause the symptom.

  Workaround: Save the current running configuration file to a temporary file in Flash memory or on a TFTP server. Reload the router. Immediately after reloading, copy the saved configuration to nvram:startup-config.

- CSCdy11785

  Symptoms: A Cisco 7206VXR may reload because of a bus error when the **show environment last** EXEC command is executed. The following error message may be displayed:

  ```
  router# show environment last
  -Traceback= 6060A0CC 60608C74 60716E90 60722340 606268FC 60634A9C 60696A9C 60696A88
  signal= 0xA, code= 0x8, context= 0x62245C90
  ```

  Conditions: This symptom is observed on a Cisco 7206VXR that is running Cisco IOS Release 12.2(2)DD4.

  Workaround: There is no workaround.

- CSCdz61503

  Symptoms: A Cisco router may reload when it performs Simple Network Management Protocol (SNMP) Notification Log MIB queries.

  Conditions: This symptom is observed on all versions of Cisco IOS software.

  Workaround: There is no workaround; however, the symptoms are not observed on a Cisco ONS 15530 or a Cisco ONS 15540 switch module because the symptoms have been resolved on these platforms.

- CSCea15879

  Symptoms: A Cisco router that is configured with Cisco Service Assurance Agent (CSAA) may run out of memory and permanently pause because the round-trip home (RTT) responder process does not free memory. This may occur when many jitter probes are sent simultaneously to the same target with the same destination port.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13) and that is configured with CSAA.

  Workaround: Try any of the following workarounds:

  Do not use the same destination port for all probes.

  Lower the probe duration.

Use the **no rtr responder** global configuration command followed by the **rtr responder** global configuration command.

- CSCea21328

  Symptoms: After a Versatile Interface Processor (VIP) has reloaded, there does not seem to be a crashinfo file because the crashinfo file is not closed; therefore, it is not visible or accessible. If the same VIP reloads again, both the first and second crashinfo files are accessible.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(6f).

  Workaround: There is no workaround.

- CSCea26010

  Symptoms: A Cisco router may reload when two port adapters are inserted in the router.

  Conditions: This symptom is observed on a Cisco 7206 router when two port adapters are inserted in the router within several seconds of each other.

  Workaround: Wait for the first inserted port adapter to come up and then insert the second port adapter.

- CSCuk38757

  Symptoms: The cardIfTable table is not correctly populated for channelized interfaces. All of the entries return a value of “ñ1”.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.0(22)S.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCea38774

  Symptoms: When the **show parser cache** EXEC command is executed, a router may reload when bringing up a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session. The reload may occur when there is more than one session accessing the parser cache and one of the sessions executes the **show parser cache** EXEC command.

  Conditions: This symptom is observed when more than one session executes the **show parser cache** EXEC command and the other session is creating the cache entry. During the creation of the cache entry when there is not enough space in the cache, old entries may be replaced with new entries and old entries may be freed. There is the possibility that freed and invalid entries may be accessed by the session that is issuing the **show parser cache** EXEC command.

  Workaround: Disable the parser cache by using the **no parser cache** global configuration command.

IBM Connectivity

- CSCdx84417

  Symptoms: A Cisco router that is doing a serial tunnel (STUN) may reload when the TCP connection is manually cleared from its peer.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10a) when a STUN peer is running and the cable is removed.

Workaround: Do not remove the cable.

- CSCdz16768

  Symptoms: After the **sdlc poll-pause-timer 10** interface configuration command is configured on a serial interface, a Cisco 2610 router that is the primary DTE sends a poll frame to a secondary DCE station at 150 msec to 180 ms intervals.

  Conditions: This symptom is observed on a Cisco 2600 series router that is running Cisco IOS Release 12.1(17).

  Workaround: There is no workaround.

- CSCdz40029

  Symptoms: Data-link switching (DLSw) may cause a buffer leak in the small buffer pool of a Cisco router.

  Conditions: This symptom is observed when DLSw Ethernet redundancy is configured and the end system starts the communication by sending an exchange identification (XID) frame to a destination service access point (DSAP) other than zero. (The symptom is not observed when the end system starts the communication by sending a test frame or an XID frame to DSAP zero.) The symptom is most likely to occur when the **dlsw timer explorer-wait-time** *time* global configuration command is configured. The larger the value of the time argument, the faster the buffers leak

  Note that the symptom does not occur when DLSw is configured with either source-bridging, transparent bridge groups, Synchronous Data Link Control (SDLC), or Qualified Logical Link Control (QLLC), but the symptom occurs only when DLSw Ethernet redundancy is configured.

  Workaround: To minimize the impact of the buffer leak, either reduce the *time* argument to 1 second or disable the **dlsw timer explorer-wait-time** global configuration command. This workaround does not completely resolve the symptom but minimizes the rate at which the buffers leak.

- CSCea29740

  Symptoms: Data-link switching (DLSw) Ethernet redundancy may not function; two routers may not be able to establish a master/slave relationship.

  Conditions: This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.2(17) and that is configured with Fast Ethernet or Gigabit Ethernet interfaces on which Inter-Switch Link (ISL) or dot1q trunking encapsulation is enabled.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCdy61602

  Symptoms: X.25 does not function as expected on channelized T1 port adapter (PA-2CT1) and channelized E1 port adapter (PA-2CE1) interfaces.

  Conditions: This symptom is observed on Cisco 7500 series routers. In addition, messages such as “output frozen” and “not transmitting” may be seen on such interfaces. This behavior may result in a CBUS complex.

  Workaround: There is no workaround.

- CSCea11453

  Symptoms: A router may reload when an interface fails and display the following error message in the log:

  ```
  %ATMPA-3-SARCRASH: ATM1/0: SAR0 Chip Crashdump:
  ```

Conditions: This symptom is observed when an interface fails on a Cisco 7200 series that has a Network Processing Engine 400 (NPE-400).

Workaround: There is no workaround.

- CSCin34068

  Symptom: Interfaces may not be created when a channel group is configured on a Cisco 7500 series or a Cisco 7600 series router.

  Conditions: This symptom is observed only if channel groups are created on an 8-port multichannel T1 port adapter (PA-MC-8T1) and the PA-MC-8T1 is replaced with an enhanced 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) by performing an online insertion and removal (OIR) procedure. After the port adapters are switched, the channel group configuration on the PA-MC-8TE1+ does not work as expected.

  Workaround: Remove the channel group configuration on a port adapter before performing an OIR and replacing the port adapter with another port adapter.

IP Routing Protocols

- CSCdw75696

  Symptoms: Issuing the **clear ip mroute *** EXEC command under heavy multicast traffic, especially Internet Group Management Protocol (IGMP) traffic, may cause a watchdog timeout, and the router may permanently pause.

  Conditions: These symptoms are observed on Cisco 7500 series and Cisco 12000 series Internet routers that are running Cisco IOS releases prior to 12.0(22)S and 12.2(16).

  Workaround: There is no workaround.

- CSCdy76664

  Symptoms: A Cisco router that is configured as a Network Address Translation (NAT) device may not correctly translate the inside address to the outside address within an H.323 signaling message.

  The following error message may be seen in the output of the **debug ip nat h323** EXEC command:

  ```
  01:16:24: NAT: H225: [0] Setup message changed, encoding back
  01:16:24: NAT: H225: newly encoded message length (118) doesn't match original length (123)
  ```

  Conditions: This symptom is observed when a Cisco Analog Telephone Adapter (ATA) 186 uses a Cisco router as a NAT device.

  Workaround: There is no workaround.

- CSCdz37639

  Symptoms: A Cisco router hangs up or permanently pauses to rommon.

  Conditions: This symptom is observed when stress reconfigurations, such as Protocol Independent Multicast (PIM) mode changes, adding or removing multicast-enabled interfaces, and clearing mroutes, result in many multicast routes being deleted and readded.

  Workaround: There is no workaround.

- CSCdz41087

  Symptoms: An interface that is defined in an Enhanced Interior Gateway Routing Protocol (EIGRP) network statement may fail to come up in the EIGRP topology table.

Conditions: This symptom is observed after a Cisco router has reloaded. The occurrence of the symptom depends on the type of interface to which the router is connected and on the timing of the interface activation.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCdz41310

  Symptoms: Memory fragmentation may occur on a router.

  Conditions: This symptom is observed when a large number of Open Shortest Path First (OSPF) routes are flapped on a Cisco router.

  Workaround: There is no workaround.

- CSCdz46435

  Symptoms: A spurious memory access may occur, and a traceback may be generated when you deconfigure Protocol Independent Multicast (PIM).

  Conditions: This symptom is observed when you deconfigure PIM from a subinterface that is configured for Frame-Relay encapsulation.

  Workaround: There is no workaround.

- CSCdz76611

  Symptoms: A router may reload when a static Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor statement is being removed.

  Conditions: If a static neighbor statement is removed from the EIGRP configuration at the same time the neighbor is going down, the router may reload.

  Workaround: Do not use static neighbors in EIGRP.

- CSCdz78549

  Symptoms: A Cisco 7401ASR router may permanently pause after the **more system: running-config** EXEC command or the **show running-config** EXEC command is issued.

  Conditions: This symptom is observed on a Cisco 7401ASR router that is configured with Stateful Network Address Translation (SNAT).

  Workaround: There is no workaround.

- CSCdz84521

  Symptoms: The Selective Packet Discard (SPD) with an IP precedence of 6 and 7 may not function correctly. Packets may be treated as nonpriority packets. The SPD is used when a queue is filling (for example, because of a flap or change) and routing traffic must be guaranteed a high priority and not dropped while the interface recovers. In this situation, routing traffic with an IP precedence of 6 and 7 is not given proper priority, and the recovery process may be delayed.

  Conditions: This symptom is observed with incoming traffic on any interface of a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCdz86780

  Symptoms: A packet to which Network Address Translation (NAT) has been applied may not be properly processed by policy-based routing (PBR).

  Conditions: This symptom is observed after NAT has been applied to a packet in the Cisco Express Forwarding (CEF) path and the packet is then sent by another feature to the process path. PBR in the process path may not handle the packet as expected because the source or destination of the packet, or both, have been changed by NAT.

Workaround: Disable CEF.

- CSCea10787

  Symptoms: A Network Address Translation (NAT) static network configuration may not function for multicast packets.

  Conditions: This symptom is observed when the **ip nat inside source** global configuration command is configured with the **static** keyword and multicast packets are being processed.

  Workaround: There is no workaround.

- CSCea14412

  Symptoms: A Cisco router receives the following error message and permanently pauses when the distribute-list * router configuration command is entered.

  ```
  System returned to ROM by bus error at PC 0x605FBA3C, address 0xEF4321D9
  ```

  Conditions: This symptom is observed in the generic IP routing table of a Cisco router. It is a day one race condition symptom. It may be observed when the CPU is under a severe load.

  Workaround: There is no workaround.

- CSCea22310

  Symptoms: A Cisco router may reload when you enter the **ip nhrp authentication** *string* interface configuration command and the *string* argument exceeds eight characters.

  Conditions: This symptom is observed on a Cisco 3662 that is running Cisco IOS Release 12.2(13)T1.

  Workaround: Limit the *string* argument to eight characters or less.

- CSCea26993

  Symptoms: Multicast traffic may get dropped by a Cisco router that is running in dense mode. (Note that all routers have the multicast group in a pruned state even though interested receivers are present.)

  Conditions: This symptom is observed when a T-flag is incorrectly set on an (S,G) entry.

  A process that is used by dense mode and that is called an Assert process (referred to as Assert) is triggered, causing a designated forwarder (referred to as an Assert winner) to be elected. The Assert winner forwards multicast traffic onto a multiaccess segment when there is more than one router on the segment. If the router that becomes the Assert winner has the T-flag incorrectly set because traffic arrives on its outgoing interface (OIF) rather than on its incoming interface (IIF), multicast traffic is dropped as a result of Reverse Path Forwarding (RPF).

  The Assert winner is based on the lowest administrative distance that is required to reach the source. When administrative distances are equal, the Interior Gateway Protocol (IGP) metric is used to determine how to reach the source. When both the administrative distance and the IGP metric are equal, the router with the highest IP address is used as a tiebreaker.

  Possible Workaround: Disable Protocol Independent Multicast (PIM) on the interface of the Assert winner that has incorrectly set the T-flag on its (S,G) entry as a result of receiving traffic on its OIF rather than on its IIF.

  First Possible Alternate Workaround: Enter the **ip mroute** *source-address rpf-address distance* global configuration command with a value of 255 for the *distance* argument on the Assert winner.

  Second Possible Alternate Workaround: Configure the **ip pim sparse-mode** interface configuration command on the interface of the Assert winner to prevent the interface from operating in dense mode.

- CSCea55449

  Symptoms: The Multilayer Switch Feature Card (MSFC) of a Cisco Catalyst 6000 may reload with the following error message:

  ```
  System was restarted by bus error at PC 0x40DFEE54, address 0xB0D0B7D
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 that is running Cisco IOS Release 12.1(13)E4 and that is configured for Network Address Translation (NAT).

  Workaround: There is no workaround.

- CSCin11611

  Symptoms: Internetwork Packet Exchange (IPX) Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors will not form adjacencies if incremental Service Advertising Protocol (SAP) updates are enabled. IPX EIGRP neighbors will not remain established and IPX routing will not work for interfaces that are affected by this symptom.

  The following message is displayed if the **eigrp log-neighbor-change** router configuration command is configured:

  ```
  %DUAL-5-NBRCHANGE: IPX-EIGRP 1: Neighbor ABC.0001.4266.3381 (Serial0/0)is down: Auth
  failure
  ```

  Incremental SAP updates are enabled by default on all non-IEEE interfaces (WAN interfaces). Incremental SAP updates are also disabled on all IEEE interfaces (LAN interfaces). Therefore, LAN interfaces are not affected by this symptom unless the interfaces have been configured to perform incremental SAP updates by entering the **ipx sap-incremental** interface configuration command.

  Conditions: This symptom is observed on a Cisco 4224 that is running Cisco IOS Release 12.2(8.05)T.

  Workaround: Configure the **no ipx sap-incremental** interface configuration command on the interfaces that have incremental SAP updates enabled by default or configuration to prevent the symptom from occurring.

- CSCin31057

  Symptoms: A router may reload when a subinterface with a certain configuration is deleted.

  Conditions: This symptom is observed on a Cisco router that has multicast and the Hot Standby Routing Protocol (HSRP) configured.

  Workaround: Remove the multicast configuration before deleting the subinterface.

Miscellaneous

- CSCds76128

  Symptoms: A Cisco router or switch may periodically display the following error message:

  ```
  %SONET-4-ALARM: POS4/11: APS disabling channel
  ```

  Conditions: This symptom is observed when an automatic protection switching (APS) protect interface is configured for PPP encapsulation. In these conditions, the above-mentioned error is message is of a cosmetic nature.

  Workaround: Change the encapsulation from PPP to High-Level Data Link Control (HDLC).

- CSCdu14815

  Symptoms: In a multiple crypto peer and tunnel environment, packets may be encrypted with the wrong security associations and delivered to the wrong peers. This symptom may coincide with the following error on the unintended crypto peers:

```
%CRYPTO-4-RECVD_PKT_INV_IDENTITY: identity doesn't match negotiated identity
```

Conditions: This symptom is observed if the encryption router is a Cisco 7100 series or a Cisco 7200 series that is configured with an Integrated Service Adapter (ISA), an Integrated Service Module (ISM), a Virtual Private Network (VPN) Acceleration Module (VAM), an IP Security (IPSec) accelerator module and that is running Cisco Express Forwarding (CEF) switching.

Workaround: Use fast switching instead of CEF switching.

- CSCdx31265

  Symptoms: Dial FTP throughput on a downlink may degrade by 18 percent.

  Conditions: This symptom is observed on a NextPort asynchronous modem interface on a Cisco AS5400 universal access gateway. The degradation in the throughput occurs because the NextPort asynchronous modem interface sends out misformatted packets on the PPP dialup link and causes retransmissions to occur with TCP-based client applications.

  Workaround: There is no workaround.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdy18970

  Symptoms: A Cisco AS5800 router may reload because of a bus error when it attempts to access an invalid address.

  Conditions: This symptom is observed on a Cisco AS5800 router that is running Cisco IOS Release 12.1(15).

  Workaround: There is no workaround.

- CSCdy20760

  Symptoms: A Cisco AS5300 may reload because of a software condition, and the following error message may be displayed when you enter the **show version** EXEC command:

  ```
  System returned to ROM by error - a Software forced crash, PC 0xXXXXXXXX
  ```

  "0xXXXXXXXX" represents the program counter on which the reload occurred.

Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.1(16) but may also occur in Release 12.2 T.

Workaround: There is no workaround.

- CSCdy24304

  Symptoms: A single-port ATM T3 network module (NM-1A-T3) or a single-port ATM E3 network module (NM-1A-E3) may stop passing traffic.

  Conditions: This symptom is observed on an NM-1A-T3 or NM-1A-E3 network module of a Cisco router.

  Workaround: Enter the **clear interface** EXEC command.

- CSCdy86668

  Symptoms: During an ISDN Multilink PPP (MLP) call, the following error message may appear on the console or in the syslog of a Cisco 3660 router:

  ```
  ALIGN-3-SPURIOUS: Spurious memory access made at 0x... reading 0x0
  ```

  Conditions: This symptom is observed on a Cisco 3660 router that is configured with a Compression Advanced Interface Module (CAIM) and that is running Cisco IOS Release 12.2(7c).

  Workaround: There is no workaround. Information about alignment errors may be found at the following location: http://www.cisco.com/warp/public/63/spuraccess.html.

- CSCdz09551

  Symptoms: The following traceback message may be displayed:

  ```
  AAAA-3-BADSTR: Bad accounting data: too many attributes:
  -Traceback= 0x604E3200 0x604E6A5C 0x60235F9C 0x601CE774 0x601CF2A0 0x601FC60C
  0x601FE804 0x601FFF08
  ```

  Conditions: This symptom is observed on a Cisco AS5350.

  Workaround: There is no workaround.

- CSCdz16414

  Symptoms: Network Time Protocol (NTP) may not remain synchronized.

  Conditions: This symptom is observed on a Cisco ONS 15104. After several minutes of operation, the clock wanders and the NTP becomes unsynchronized.

  Workaround: Unconfigure and then reconfigure the NTP configuration to enable the NTP to synchronize again until the symptom reoccurs.

- CSCdz20801

  Symptoms: A Cisco AS5850 may reload because of a memory corruption.

  Conditions: This symptom is observed on a Cisco AS5850 that is functioning as a voice gateway and that is running Cisco IOS Release 12.2(11)T2.

  Workaround: There is no workaround.

- CSCdz23373

  Symptoms: A Parallel Express Forwarding (PXF) exception may occur when a very large access control list (ACL) is configured.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(12a) and that is configured with a Network Services Engine 1 (NSE-1).

  Workaround: If you can work without PXF, disable PXF using the **no ip pxf** global configuration command. However, if you must use PXF, there is no workaround.

- CSCdz40483

  Symptoms: A Cisco router permanently pauses with a watchdog timer under normal operation.

  Conditions: This symptom is observed when the router is a voice endpoint with active calls.

  Workaround: There is no workaround.

- CSCdz50199

  Symptoms: When the **service-policy** interface configuration command has been configured on any of its interfaces, a Cisco router may reload during the bootup process, and the following error message is logged on the console of the router:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0xABCD, ra=0xFJHK, sp=0xLMNOPQRS
  ```

  Note: Pc represents the program counter; ra represents the return address; sp represents the stack pointer.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(15) or Release 12.2(15)T.

  Workaround: Disable the configuration of the service policy before you reload the router and reapply the configuration of the service policy after the router has been booted up.

- CSCdz58142

  Symptoms: A block serial tunnel (BSTUN) Binary Synchronous Communications (Bisync) connection to several ATMs pauses sporadically.

  Conditions: This symptom is observed on a Cisco 3662 router that is running Cisco IOS Release 12.2(12a) and that is configured with NM-2W and WIC-2T cards as the DTE. This symptom applies to all WICs in NM-xFE-2W modules. It includes the NM-2W, NM-1FE-2W, NM-2FE-2W, and NM-1R-1FE-2W modules as they all have the DSCC4 serial communications controller on them.

  A **show interface serial x/y** EXEC command on the Bisync interface shows that input packets increment slowly, but output packets have stopped incrementing.

  A **show controller serial x/y** EXEC command on the Bisync interface shows that tx interrupts do not continue to increment, but indicates that the transmitter is paused on the serial interface.

  A **debug bsc packet** EXEC command executed during the pause shows the following output:

  ```
  %BSC-3-BADLINESTATE: Line state Tx when receiving INVALID on line Serial3/1
  %BSC-3-BADLINESTATE: Line state Tx when receiving INVALID on line Serial3/1
  %BSC-3-BADLINESTATE: Line state Tx when receiving INVALID on line Serial3/1
  %BSC-3-BADLINESTATE: Line state Tx when receiving INVALID on line Serial3/1
  %BSC-3-BADLINESTATE: Line state Tx when receiving INVALID on line Serial3/1
  ```

  or

  ```
  %BSC-3-BADLINESTATE: Line state Tx when receiving EOT on line Serial3/0
  %BSC-3-BADLINESTATE: Line state Tx when receiving PLSL on line Serial3/0
  %BSC-3-BADLINESTATE: Line state Tx when receiving EOT on line Serial3/0
  %BSC-3-BADLINESTATE: Line state Tx when receiving PLSL on line Serial3/0
  %BSC-3-BADLINESTATE: Line state Tx when receiving EOT on line Serial3/0
  ```

  Workaround: Use the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected serial interface.

- CSCdz60807

  Symptoms: When you enter the **use-proxy** gatekeeper configuration command, a Cisco router may reload because of a bus error.

Conditions: This symptom is observed only when calls are handled by the Multimedia Conference Manager (MCM) proxy. The symptom is related to the H.245 facility message; if the endpoints do not generate facility messages, the symptom does not occur.

Workaround: Disable the MCM proxy.

- CSCdz66927

  Symptoms: Voice ports on a router may be stuck in a seizure acknowledgement (SEIZURE-ACK) state.

  Conditions: This symptom is observed for a number of calls on voice ports because some digits in the calls are not pulsed out.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to clear the voice ports.

- CSCdz69000

  Symptoms: A Versatile Interface Processor 4-80 (VIP4-80) may reload during normal operation.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2 or Release 12.2 T when Real-Time Transport Protocol (RTP) and distributed switching are enabled.

  Workaround: Disable distributed switching using the **no ip cef distributed** global configuration command.

- CSCdz69177

  Symptoms: A spurious memory access may occur on the Versatile Interface Processor (VIP) of a Cisco 7500 series even though the RSP/VIP is not crashing.

  Conditions: This symptom is observed when Multiprotocol Label Switching (MPLS) forwarding is enabled.

  Workaround: There is no workaround.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCdz71295

  Symptoms: Poor voice quality occurs after several calls on a Cisco router.

  Conditions: This symptom is observed on a Cisco 7500 series router that is configured with Compressed Real-Time Protocol (CRTP) header compression.

  Workaround: Disable the CRTP.

- CSCdz76166

  Symptoms: A Cisco router may reload after execution of the **show atm vc** *vcd* EXEC command.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(15) or a later release, and that has an ATM interface. The *vcd* value should correspond to a switched virtual circuit (SVC).

Workaround: There is no workaround.

- CSCdz78239

  Symptoms: A Cisco 7100 or Cisco 7200 series router with the Integrated Service Module (ISM) card and Integrated Service Adapter (ISA) adapter intermittently resets.

  Conditions: This symptom is observed on a Cisco 7100 and Cisco 7200 series router that is configured with an ISA adapter and ISM card and that is running Cisco IOS Release 12.1(14)E.

  After the ISA card reset message is displayed, the following occurs:

  Some of the IPsec tunnels pause intermittently.

  The **show crypto ipsec sa** EXEC command shows that the IPSec security associations (SAs) are running, but no encryption or decryption occurs.

  Sometimes the router pauses immediately after the ISA card reset.

  Workaround: There is no workaround.

- CSCdz79023

  Symptoms: An ATM subinterface that is configured with switched virtual circuits (SVCs) may pause indefinitely and does not recover.

  Conditions: This symptom is observed when the last dynamic virtual circuit (VC) is deleted from the interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCdz79996

  Symptoms: TCP retransmissions may occur on a router after the Web Cache Communication Protocol (WCCP) is enabled.

  A sniffer trace indicates that some packets that should be redirected to a content engine via WCCP are not delivered as expected. This behavior causes the retransmissions to occur between the client and the caching device. When this symptom occurs, clients may not be able to view certain web pages for several minutes.

  Conditions: This symptom is observed on a Cisco 7206VXR that has WCCP and Cisco Express Forwarding (CEF) enabled. Network address translation (NAT) from the inside to the outside is occurring on the Internet interface that has an outbound access control list (ACL) configured. If the outbound ACL contains statements that deny traffic with internal non- NAT addresses, those packets will not be redirected because WCCP in the CEF path checks to ensure that packets are permitted to pass through the original outbound interface before applying redirection to the packets.

  Because the check is performed on packets before NAT is applied the packets are not redirected. From the perspective of a client, web pages may become unreachable when this symptom occurs. However, if a packet is switched in the fast path rather than the CEF path, then the check against any ACL that is configured on the original outbound interface is not made and redirection occurs normally.

  Workaround: Configure the ACL on the original outbound interface so that it does not deny packets that must be redirected. When you are configuring the ACL, remember that NAT would not have been applied to redirect candidates when the ACL is checked.

- CSCdz81619

  Symptoms: Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic may be dropped as ignored traffic.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2 when all the following conditions are present:

  - The router is configured for distributed Cisco Express Forwarding (DCEF).
  - The MPLS VPN traffic enters via a Gigabit Ethernet (GE) subinterface that has dot1q encapsulation enabled.
  - The MPLS VPN traffic leaves via a VPN routing/forwarding (VRF) subinterface that has dot1q encapsulation enabled.
  - Both the GE ingress subinterface and the VRF egress subinterface belong to the same main interface.

  The number of "ignored" in the output of the **show interfaces** privileged EXEC command should match the "ChkSum_Err" field in output of the **show cef drop** EXEC command or the checksum error information in the output of the **show ip traffic** EXEC command.

  Workaround: Do not use DCEF; rather, use CEF.

- CSCdz84025

  Symptoms: A router will permanently pause as soon as the Cisco IOS software that has a code fix for the caveat CSCdz77618 is loaded. The following error message will occur as soon as the software image is loaded:

  ```
  *CWTLC PXF crash:Internal Error (0x00210001): Col0 CRASH_CODE_CMD_ID
  ```

  Conditions: This symptom is observed on all ethernet cards for the Cisco 7500 series routers.

  Workaround: There is no workaround.

- CSCdz85565

  Symptoms: A Cisco 7200 series router will cause IP Header Compression (IPHC) regression test failures.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.02(14.01). Because fast-switched packets are counted as process-switched packets, the symptom is observed only on M4T interfaces.

  Workaround: There is no workaround.

- CSCdz85922

  Symptoms: A Cisco 7500 series router or a Cisco 12000 series Internet router may experience a reload of either the Versatile Interface Processor (VIP) or the line card and display the following message:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = TFIB Stats Background
  ```

  Conditions: These symptoms may affect only Cisco IOS releases with the fix for the caveat CSCdz32988 and only platforms that perform distributed Multiprotocol Label Switching (MPLS) forwarding. Cisco IOS releases that may contain these symptoms include Release 12.0(21)S, Release 12.0(22)S, Release 12.0(23)S, Release 12.1 and its derivatives, and Release 12.2 mainline. Cisco IOS Release 12.2 T and the latest Cisco IOS Release 12.0 S software are not susceptible to these symptoms.

  Workaround: There is no workaround.

- CSCdz88297

  Symptoms: A Systems Network Architecture Switching Services (SNASw) router may stop forwarding BIND and UNBIND requests.

  Conditions: This symptom is observed after the SNASw router receives an activate logical unit (ACTLU) request that is forwarded to a downstream physical unit (DSPU). This symptom will occur if the DSPU sends the ACTLU response back to the SNASw router without setting the response bit in the SNA request and resources header (RH).

  Workaround: Restart the SNASw router.

- CSCdz88368

  Symptoms: A nonexistent policy may that is configured as the input or output service policy of an ATM virtual circuit (VC) causes a router to be unable to display or save its configuration.

  Conditions: This symptom is observed Cisco Route Processor Module (RPM) routers, but may affect any Cisco router that is using ATM interfaces.

  Workaround: Do not specify nonexistent policy maps as an ATM VC service policy.

- CSCdz89370

  Symptoms: High-speed interfaces that have a speed of 428 Mbps or higher cannot be configured with certain quality of service (QoS) features that can be configured with the rate parameter.

  Conditions: This symptom is observed on a Cisco 7500 series when high-speed interfaces that have a speed of 428 Mbps or higher are configured with QoS features that can be configured with the rate parameter.

  Workaround: There is no workaround.

- CSCea00475

  Symptoms: A generic routing encapsulation (GRE) tunnel that carries Frame Relay (FR) packets may not remove the padding (if any) of the original packets upon decapsulation. This behavior results in the padding being sent out with the FR packets instead of being removed.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(11.2), Release 12.2(11.2)S, and Release 12.2(11.3)T.

  Workaround: There is no workaround.

- CSCea01472

  Symptoms: A Versatile Interface Processor 2-50 (VIP2-50) may reload after it boots up.

  Conditions: This symptom is observed on a VIP2-50 that has a 1-port multichannel E3 port adapter (PA-MC-E3) that has distributed link fragmentation and interleaving (LFI) with Virtual Private Network routing and forwarding (VRF) configured on its interfaces.

  Workaround: There is no workaround.

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea02713

  Symptoms: A router may unexpectedly reload if it is unable to allocate enough memory for Weighted Random Early Detection (WRED). This unexpected reload may also be seen when the interface is already configured for WRED by using modular quality of service (QoS) and when an access group is added to the interface.

  Conditions: This symptom is observed on a router that is running Cisco IOS software that is being configured for WRED on a Frame Relay interface via the modular QoS.

  Workaround: There is no workaround.

- CSCea02744

  Symptoms: The **ignore-dcd** interface configuration command does not allow an interface to come up when it is connected to a device that sends a data set ready (DSR) signal instead of a data carrier detect (DCD) signal. The interface will remain in the up/down state.

  Conditions: This symptom is observed on a 1-port serial WAN interface card (WIC-1T) or a 2-port serial WAN interface card (WIC-2T) that is installed on a 1-port Fast Ethernet network module with two WAN card slots (NM-1FE2W) or a 2- port Fast Ethernet network module with two WAN card slots (NM-1FE2W or NM- 2FE2W) on a Cisco 2600 series, Cisco 3600 series, or Cisco 3700 series that is running Cisco IOS Release 12.2(13)T.

  Workaround: To enable the interface to come into the up/up state, shorten the DSR signal to a DCD signal using a breakout device.

- CSCea04706

  Symptoms: A Cisco AS5300 has calls failing with the following error message:

  ```
  íservice/option not availableí cause coe=0x3F
  ```

  Conditions: This symptom is observed on the digital signal processors (DSPs) on the voice feature card (VFC). The router is in the state “DSPRM-PLATFM: resource recovery” because of dangling DSPs.

  Workaround: Recover the DSPs to reduce the effect.

- CSCea06647

  Symptoms: Use of the **dir** (directory) command at the router command prompt fails to list files stored on an Advanced Technology Attachment (ATA) Flash card. However, an equivalent command on a PC lists the stored files.

  Conditions: This symptom is observed on an ATA Flash card that has been formatted as FAT16 in a PC that is running Windows 2000. The card can no longer be read or reformatted under Cisco IOS software.

  Workaround: Reformat the ATA Flash card as FAT16 on a PC that is running Windows 95 or Windows 98.

- CSCea07020

  Symptoms: A Cisco router that is configured with Frame Relay (FR) subinterfaces may leak memory if the subinterfaces are configured with Random Early Detection (RED).

  Conditions: This symptom is observed when traffic shaping is configured with RED configured in the subclass in the service policy. If the subinterfaces are configured with RED, other changes to the configuration may cause the router to leak memory as well. For instance, adding an IP access list to a Frame Relay subinterface that is configured with RED will cause the router to leak memory.

  Workaround: There is no workaround.

- CSCea07557

  Symptoms: The selective packet discard (SPD) feature does not function correctly on the E0 interface of a Cisco AS5300 router.

  Conditions: This symptom is observed on a Cisco AS5300 router.

  Workaround: Increase the input hold queue.

- CSCea07570

  Symptoms: A Route Switch Processor (RSP) may reload.

  Conditions: This symptom is observed when an RSP is sending Multiprotocol Label Switching (MPLS) packets over a Multilink PPP (MLP) interface.

  Workaround: Use dCEF, this problem is specific to RSP switching.

- CSCea07778

  Symptoms: A router may reload while a virtual private dial-up network (VPDN) connection is being established. The VPDN connection is copied from a virtual template, and the callback is enabled on the VPDN.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(15.1).

  Workaround: Use dialer profiles. This workaround has limited scope because dialer profiles are not scalable.

- CSCea09001

  Symptoms: Systems Network Architecture switching services (SNASw) logical units (LUs) may fail to establish a session with their virtual telecommunications access method (VTAM) application. The session fails with sense code 0855000F, which indicates the following information:

  ```
  Route Setup procedure failure: An intermediate or destination node was unable to
  successfully complete the processing of a high-performance routing (HPR) Route Setup
  request or reply.

  The route setup request completed unsuccessfully. The route setup reply was not
  received in the allotted time (as determined by the IOPURGE start option).
  ```

  Conditions: This symptom is observed when the SNASw router is connected upstream via High-Performance Routing (HPR)/IP links to two network nodes (NNs) and occurs after repeated Logical Data Link Control (LDLC) timeouts occur and “RSETUP” HPR pipe timeouts occur upstream to an NN.

  Further Details 1: SNASw receives the route-setup request via the RSETUP HPR pipe and sends its route-setup reply via Intermediate Session Routing (ISR) back to the VTAM NN. However, the VTAM does not receive the route-setup reply, and consequently the session fails with a sense code 0855000F.

  The symptom occurs when both NNs activate the RSETUP Rapid Transport Protocol (RTP) connection at the same time. Note that this is a valid condition with two active RSETUP RTP connections, one in each direction. However, because these RTP connections are independent, one connection may time out and be deactivated while the other may continue to be active. When the RSETUP connection that is activated by SNASw times out first, the SNASw router continues to receive route-setup requests on the other RSETUP connection. SNASw then attempts to send the route-setup replies as non-RTP data, but these replies are discarded. Eventually the remaining RTP connection times out at the remote node.

Further Details 2: When SNASw (CPNAME SNASW001) receives a route-setup request general data stream (GDS) variable (x'12CE') on an RSETUP HPR pipe from "NETWORKA.MVSBBB" while the origin of the route-setup request was "NETWORKA.MVSAAA," the output of the **snasw dlctrace** global configuration command displays the following information:

```
34191  MVSLINKB In  sz:203  HPR RtSetup
TCID(E A7000000)  DL(A6) BSQ(1EF27) SR SM EM ARB(RQ)
   0000 C60880FF 00000000 0EA70000 003C0400  *F........x......*
   0010 08000000 A60001EF 27032281 50004EDD  *....w......a&.+.*
   0020 A0000000 0000A612 CE000200 00000000  *......w.........*
   0030 00000000 00140EF3 D5C5E3E6 D6D9D2C1  *.......3NETWORKA*
   0040 4BC4E3E5 F1F1F0F0 F9342B02 021A4618  *.DTV11009.......*
   0050 80150FD5 C5E3E6D6 D9D2C14B D4E5E2C2  *...NETWORKA.MVSB*
   0060 C2C22100 00002516 46118015 08E2D5C1  *BB..........SNA*
   0070 E2E6F0F0 F1218000 00250388 800A2C02  *SW001......h....*
   0080 067BC9D5 E3C5D91A 60FE63CD 2E72D562  *.#INTER.-.....N.*
   0090 190FD5C5 E3E6D6D9 D2C14BD4 E5E2C1C1  *..NETWORKA.MVSAA*
   00A0 C12A8040 00000005 A7000001 5000000F  *A.. ....x...&...*
   00B0 A0000000 0016670A 00807900 66000000  *..........`.....*
   00C0 000A0080 6404A400                    *......u.        *
```

When SNASW001 sends back an HPR status segment acknowledging the receipt of the route-setup request, the output of the **snasw dlctrace** global configuration command displays the following information:

```
34192  MVSLINKB Out sz:64   HPR      Stat Rpy ARB
TCID(2BF94FB8 8BC)  DL(0) BSQ(0) ST(1EFCE) ARB(RP)
   0000 C600D200 00000000 0000FF00 2BF94FB8  *F.K..........9..*
   0010 000008BC 0004000D 00000000 00000000  *................*
   0020 050E0000 00000234 0001EFCE 00000000  *................*
   0030 00000000 03224105 00000000 00000000  *................*
```

When SNASW001 generates the route-setup reply GDS and sends it back to NETWORKA.MVSAAA via NETWORKA.MVSBBB and via ISR, the output of the **snasw dlctrace** global configuration command displays the following information. (Note that NETWORKA.MVSBBB probably does not receive this route-setup reply because the reply should be sent via the HPR RSETUP pipe on which the route-setup request is received.)

```
34193  MVSLINKB Out sz:184  ISR Rq RtSetup
   0000 2D000000 00002B00 001000AE 12CE9002  *................*
   0010 A0000001 D4C00000 00000A2C 02067BC9  *....M{........#I*
   0020 D5E3C5D9 1A60FE63 CD2E72D5 62190FD5  *NTER.-.....N...N*
   0030 C5E3E6D6 D9D2C14B C9C4E2D7 C9C12A80  *ETWORKA.IDSPIA..*
   0040 40000000 05A70000 01500000 0FA00000  * ....x...&......*
   0050 00001667 0A008079 00660000 00000A00  *.......`........*
   0060 806404A4 00000000 1A2B0100 16461480  *...u.....+.....*
   0070 150FD5C5 E3E6D6D9 D2C14BD4 E5E2C2C2  *..NETWORKA.MVSBB*
   0080 C221140E F4C9C4C3 D5C5E3E6 D24BE2D5  *B...4NETWORKA.SN*
   0090 C1E2E6F0 F0F10326 800639C2 10ECC819  *ASW001.....B..H.*
   00A0 80C00000 0005AA00 00004B00 003E6600  *.{..............*
   00B0 00000005 67030091                    *.......j        *
```

Workaround: First terminate the SNASw link on which the route-setup request is received; then, restart the same link; enter the **snasw stop link** *link-name* privileged EXEC command followed by the **snasw start link** *link-name* privileged EXEC command.

The resolution for this caveat ensures that if either one of the RSETUP RTP connections fails, processing continues as if there were only one RTP connection. The resolution for this caveat also resolves a minor memory leak, in which a buffer was lost every time an RSETUP or control point-to-control point (CP-CP) RTP connection was disconnected.

- CSCea09674

  Symptoms: All calls are dropped immediately when the **busyout** *slot* EXEC command is issued on a channelized T3 (CT3) dial feature card (DFC).

  Conditions: This symptom is observed on a Cisco AS5400 router that has a CT3 DFC in use and that has active dial modem calls.

  Workaround: Use the **busyout** *slot* EXEC command on all NextPort (NP 108) DFCs, the **busyout** *port* EXEC command, the Software Port Entity (SPE) **busyout** EXEC commands, or other **busyout** EXEC commands to clear calls gracefully without using the **busyout** *slot* EXEC command where the CT3 DFC is located.

- CSCea10024

  Symptoms: A Cisco 7200 series router that is configured with Systems Network Architecture Switching Services (SNASw) and enterprise extender uplinks to a mainframe permanently pauses during the mainframe initial program load (IPL). The **show proc** cpu EXEC command indicates that the router is at 99 percent CPU utilization during the IPL.

  Conditions: This symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCea11008

  Symptoms: A Versatile Interface Processor (VIP) may reload.

  Conditions: This symptom is observed on a Cisco 7500 series if there is a quality of service (QoS) service policy attached to a virtual interface that has the priority feature enabled and if that virtual interface is in the “down” state.

  Workaround: There is no workaround.

- CSCea11344

  Symptoms: The **atm abr rate-factor** interface configuration command cannot be configured on an interface.

  Conditions: This symptom is observed when an available bit rate (ABR) connection is added to a Route Processor Module-PRemium (RPM-PR) card on a Cisco MGX 8850 Processor Switch Module (PXM1) card that has Cisco WAN Manager (CWM) carrier module (CM) or when you configure the **atm abr rate- factor** interface configuration command under the interface.

  Workaround: Use the command-line interface to add an ABR connection to the RPM- PR on the Cisco MGX 8850 PXM1 card.

- CSCea12346

  Symptoms: The **show policy interface** EXEC command may display incorrect bandwidth allocation among child classes if the class is configured with the **bandwidth percent** policy-map class configuration command or the **priority percent** policy-map class configuration command.

  Conditions: This symptom is observed when a hierarchical service policy is applied to a Frame Relay map class.

Workaround: There is no workaround.

- CSCea14557

  Symptoms: After a terminating PBX sends a setup acknowledgement (SETUP_ACK) message with a Progress Indicator (PI) with the value 8, there is no dial tone.

  Conditions: This symptom is observed on a terminating gateway that is connected to an ISDN PBX. The gateway may not process the SETUP_ACK message with the PI with the value 8. The ISDN PBX sends the SETUP_ACK message in response to a setup (SETUP) message that does not include a "called number."

  The PI with the value 8 is to provide the dial tone and collect the digits.

  Workaround: There is no workaround.

- CSCea17870

  Symptoms: When Parallel Express Forwarding (PXF) is enabled, a variety of symptoms may occur depending on the Cisco router or switch:

  - A router may reload.
  - A router may not forward packets correctly.
  - The "IPFAST-2-PAKSTICK: Corrupted pak header" error message may be generated.

  Conditions: This symptom is observed when a packet is punted to the Route Processor (RP) and occurs because the paktype was not properly scrubbed after its last use.

  Workaround: Disable PXF. If this action is not an option, there is no workaround.

- CSCea21073

  Symptoms: High Performance Routing (HPR) disruptions may occur when you transfer large files.

  Conditions: This symptom is observed in an HPR IP network when there is heavy data traffic and when significant loss of packets occurs.

  Workaround: There is no workaround.

- CSCea24835

  Symptoms: A service policy that is attached to an interface without any priority feature and traffic is flowing through existing classes of that policy, stops traffic flowing through the other classes when adding the priority feature in that policy.

  Conditions: This symptom is observed when the interface that has the output service policy is congested when the priority feature is added to the policy map.

  Workaround: Remove and reattach the service policy to the interface.

- CSCea25697

  Symptoms: About 100 KB to 1 MB of processor memory may be lost when the **default interface** global configuration command is entered on a router. The memory loss can be detected by comparing the output of the s**how memory** EXEC command by entering the **show memory** EXEC command both before and after the **default interface** global configuration command is configured on the router.

  Conditions: This symptom occurs only if the **default interface** global configuration command is configured on a router.

  Workaround: The memory loss can be avoided by unconfiguring interfaces manually using the no form of the interface configuration commands.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea28471

  Symptoms: A Versatile Interface Processor (VIP) may reload.

  Conditions: This symptom is observed on a VIP if Multiprotocol Label Switching (MPLS), Egress Netflow, and distributed Cisco Express Forwarding (dCEF) are configured.

  Workaround: Disable dCEF or the Egress Netflow.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at
http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea33288

  Symptoms: A Cisco router may reload when you remove a service policy by entering the **no service-policy input** *policy-map-name* interface configuration command.

  Conditions: This symptom is observed during performance tests while traffic is flowing through the router and marking action is configured in the policy map. The symptom is platform independent.

  Workaround: There is no workaround.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea37647

  Symptoms: Duplex settings on a port channel may not be propagated onto member interfaces.

  Conditions: This symptom is observed when you change the duplex settings by using the **duplex half** or **duplex full** interface configuration command. The symptom is not observed when you change the duplex setting by suing the **half-duplex** or **full-duplex** interface configuration command.

  Workaround: Use the **half-duplex** or **full-duplex** interface configuration command to change the duplex settings.

- CSCea38803

  Symptoms: A Route Processor (RP) may reload when a member is removed and added from one multilink group to another using distributed link fragmentation and interleaving (dLFI).

Conditions: This symptom has been observed when a member link from a different bay or Flex WAN is added to the multilink interface.

It may be possible to prevent the reload of the RP by shutting down the multilink interface and making a multilink span across line cards or different bays of the Flex WAN. However, this action is not a Cisco supported configuration for distributed Multilink PPP (MLP) or dLFI.

Workaround: There is no workaround.

- CSCea38967

  Symptoms: A Cisco 7200 series or Cisco 7500 series router may reload because packet cleanup is not performed completely in the interrupt path of the High- Speed Serial Interface (HSSI) port adapter (PA).

  Conditions: This symptom is observed on a Cisco 7200 series or Cisco 7500 series.

  Workaround: Turn off Parallel Express Forwarding (PXF) with the **no ip pxf** global configuration command.

- CSCea39354

  Symptoms: A Cisco router may reload when you send a Server Load Balancing (SLB) ping through an ATM interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.2 T.

  Workaround: There is no workaround.

- CSCea42298

  Symptoms: The E3 controller of a Multi-Channel E3 port adapter (PA-MC-E3) card is missing from IF-MIB and DS3-MIB.

  Conditions: This symptom is observed on a PA-MC-E3 in all releases of Cisco IOS software.

  Workaround: There is no workaround.

- CSCea44554

  Symptoms: A Cisco gateway general packet radio service (GPRS) support node (GGSN) reloads with a bus error while updating fast cache.

  Conditions: This symptom is observed on a Cisco GGSN when fast switching is enabled and a “delete pdp (Protocol Data Packet) context” request is received.

  Workaround: There is no workaround.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea50942

  Symptoms: The **set qos-group** QoS policy-map configuration command may not function on a Multiprotocol Label Switching (MPLS) provider (P) router, and the counter for marked packets may overflow.

  Conditions: These symptoms are observed on a Cisco 7500 series that is functioning as an MPLS P router when the **set qos-group** QoS policy-map configuration command is configured for use in an incoming policy map that is applied to an ATM point-to-point virtual circuit (VC).

  Workaround: There is no workaround.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml

- CSCea60815

  Symptoms: Downstream Systems Network Architecture switching services (SNASw) physical units (PUs) may be stuck in the "PendActPu" state.

  Conditions: This symptom is observed after an initial program load (IPL) has occurred on the host.

  Workaround: Stop and restart SNASw.

- CSCea62116

  Symptoms: A Systems Network Architecture Switching Services (SNASw) router that is configured with the **snasw ipstrace** global configuration command may reload.

  Conditions: This symptom is observed when the **show snasw ips user** EXEC command is entered immediately after the **show snasw link user** EXEC command is entered.

  Workaround: Do not configure the **snasw ipstrace** global configuration command. Always use the **snasw start ipstrace user** EXEC command and the **snasw stop ipstrace user** EXEC command in conjunction with the **snasw ipstrace** global configuration command.

- CSCea64751

  Symptoms: A Cisco 2600 series may unexpectedly reload, or report "badshare" tracebacks, or do both. When the router reloads, the router generates messages similar to the following:

  ```
  Unexpected exception to CPUvector 1200, PC = 818C8B80

  -Traceback= 818C8B80 818C9454 818C9848 818CD814 818CA814 818C7A28 818BC7B4 801E64B8
  801E5D30 801D9A44 804F8CBC 8047FD74 804EB824 804EB824 8047FE34 804EBCC0
  ```

  When "badshare" tracebacks occur, the router generates messages similar to the following:

  ```
  %SYS-2-BADSHARE:Bad refcount in pak_enqueue, ptr=8316E0F8, count=0

  -Traceback= 80406718 80407C38 818CC900 8026A9A0 80271EC4 8002258C 804FB374 804F8C84
  8047FD74 804EB824 804EB824 8047FE34 80651388

  %SYS-2-BADSHARE:Bad refcount in datagram_done, ptr=8316E0F8, count=0

  -Traceback= 80403848 80407E68 818CC900 8026A9A0 80271EC4 8002258C 804FB374 804F8C84
  8047FD74 804EB824 804EB824 8047FE34 80651388

  %SYS-2-BADSHARE:Bad refcount in datagram_done, ptr=8316E0F8, count=0
  ```

  Conditions: These symptoms are observed when the following two conditions occur:

  - The Cisco 2600 series is configured with an asymmetric digital subscriber line (ADSL) or symmetric high-bit rate digital subscriber line (SHDSL) WAN interface card (WIC) that is installed in an onboard slot such as slot 0/0 or slot 0/1.
  - The upstream traffic rate exceeds the line rate, and this traffic is routed through the ADSL or SHDSL WIC. (The line rate is the maximum speed allowed by the digital subscriber line access multiplexer [DSLAM]).

  Workaround: Do not use onboard slots.

  Alternate workaround: Ensure that the router traffic rate is below the line rate.

- CSCea70473

  Symptoms: A memory leak may occur in the PPP authorization process on a Cisco 7206VXR.

  Conditions: This symptom is observed on a Cisco 7206VXR that is running Cisco IOS Release 12.2(16) and that is configured for PPP over Ethernet (PPPoE). The symptom may occur on any Cisco router that is running Cisco IOS Release 12.2(16).

  Workaround: There is no workaround.

- CSCea71681

  Symptoms: A downstream physical unit (PU) may pause indefinitely in the "Pend ACTPU" state.

Conditions: This symptom is observed on a Systems Network Architecture (SNA) switch after a host initial program load (IPL) occurs when the SNA switch is busy activating PUs. The SNA switch does not send a REQACTPU response to the dependent logical unit server (DLUS).

Workaround: Redirect the PU to a redundant SNA switch.

Alternate Workaround: Stop and restart the SNA switch.

- CSCea81256

  Symptoms: The Transparent Common Channel Signaling (T-CCS) frame forwarding connection does not work correctly on a Cisco router that is configured with a digital voice port adapter (PA).

  Conditions: This symptom is observed when one router has a VXC-2TE1+ digital voice PA and the other router has a PA-MCX-RTE1 digital voice PA, and the routers are running Cisco IOS Release 12.2(a) or later releases.

  Workaround: Run Cisco IOS Release 12.2 T on the router with the PA-MCX card.

- CSCea93882

  Symptoms: If Cisco Express Forwarding (CEF) is disabled, a router may reload with the following error message upon the receipt of a malformed generic routing encapsulation (GRE) packet:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0xA30, pc=0x40992D3C,
  ra=0x405E64B8, sp=0x43562838
  ```

  Conditions: This symptom is observed on a Cisco router that has CEF disabled. The symptom even occurs without a tunnel configuration on the router.

  Workaround: Enable CEF on the router by entering the **ip cef** global configuration command.

- CSCeb00104

  Symptoms: When configuration changes are made, a Cisco 7500 series Versatile Interface Processor (VIP) may pause indefinitely, produce large numbers of spurious memory accesses or reload. This situation may cause the router to detect that interfaces on the VIP are not sending packets and to report that the output of the interfaces is stuck.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for fragmentation and shaping on a Frame Relay interface using modular QoS CLI (MQC).

  Workaround: Before you make quality of service (QoS) policy or Frame Relay fragmentation changes on an interface of the VIP, enter the **shutdown** interface configuration command on the interface.

- CSCin22343

  Symptoms: A Cisco router that is running a GPRS gateway support node (GGSN) image, GGSN may reload in case of high PPP-PDP creates, when we are getting ip address from dhcp at rate more than 10pps

  A Cisco router that is configured with a general packet radio service (GPRS) Gateway Support Node (GGSN) may reload.

  Conditions: This symptom is observed on a Cisco router that is configured with GGSN and is receiving IP addresses by way of Dynamic Host Configuration Protocol (DHCP) at a rate greater than 10 pps.

  Conditions: When we send around 8k ppp pdp terminating at ggsn (with dhcp) with the rate of more than 10pps. After creating more than 5k sessions, all the sessions will go down due to high cpu utilization up to 100%. During this process or doing a **clear gprs gtp pdp-context all** at this stage may reload the GGSN.

  Workaround: Reduce the rate and get the IP address from the RADIUS.

- CSCin31870

  Symptoms: When you remove a Gigabit Ethernet port adapter (PA-GE) from a Cisco 7200 series and then reinsert it, the interface state is "up/up," even though there are no cables attached to the Gigabit Interface Converters (GBICs) of the PA-GE.

  Conditions: This symptom is observed after you enter the **no shutdown** interface configuration command to bring up the interface.

  Workaround: There is no workaround.

- CSCin33334

  Symptoms: A Cisco router that is configured for E1 R2 noncompelled signaling may not allow calls to be completed.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for E1 R2 noncompelled signaling. Calls are completed if the router is configured for R2 compelled signaling or R2 semicompelled signaling.

  Workaround: There is no workaround.

- CSCin34382

  Symptoms: A Cisco 7200 series or a Cisco 7401 router may reload because of a bus error exception.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Service Engine-1 (NSE-1) and on a Cisco 7401 when Parallel Express Forwarding (PXF) is enabled. This symptom occurs when the router forwards traffic through a 1-port Fast Ethernet port adapter or through a Fast Ethernet I/O controller and when moderate bi-directional traffic is running.

  Workaround: There is no workaround.

- CSCin41495

  Symptoms: After digital signal processors (DSPs) are configured on a Cisco router, the corresponding controllers cannot be located. The command-line interface (CLI) does not allow the correct controllers to be selected.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with DSPs.

  Workaround: There is no workaround.

- CSCuk41908

  Symptoms: Redirection may occur unexpectedly on a Cisco router when redirect is configured on more than one interface with more than one service configured.

  Conditions: This symptom is observed on a Cisco router when Web Cache Communication Protocol (WCCP) input redirection is configured on several interfaces and not all services are configured on each interface. In this situation, packets are matched against all services when looking for redirect candidates. This behavior may lead to a spurious match and unexpected redirection of packets to a cache.

  Workaround: Use output redirection.

Novell IPX, XNS, and Apollo Domain

- CSCdz18119

  Symptoms: A Cisco 3640 router may reload at "__doprnt."

Conditions: This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(12.14b) while the router is being configured for Internetwork Packet Exchange (IPX) routing.

Workaround: There is no workaround.

- CSCea66127

  Symptoms: IPX Enhanced Interior Gateway Routing Protocol (EIGRP) discovery packets may be stuck in the input queue and wedge the queue.

  Conditions: This symptom is observed on a Cisco router that has IPX EIGRP enabled and is sending the packets to a remote router that does not have IPX EIGRP enabled. The symptom occurs because the remote router is misconfigured.

  Workaround: Enable IPX EIGRP on the remote router.

Protocol Translation

- CSCdz37602

  Symptoms: A Cisco router may incorrectly allow the **login** keyword to be specified on a translate command when translating from an X.25 permanent virtual circuit (PVC). Deletion of the misconfigured translate command may cause the router to reload.

  Conditions: This symptom is observed when removing a translate statement that specifies an X.25 PVC as the incoming connection and that requires a login when the incoming connection is established. This combination of options is permitted but is not valid.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCdv54170

  Symptoms: The asynchronous queue manager (of the asynchronous call queueing feature) fails to release the queued position even though the connection no longer exists.

  Conditions: This symptom is observed when a connected user terminates the queued rotary connection. This condition prevents calls that are queued after the disconnected call from moving up in the queue and eventually into a free rotary line. The calls that are queued are paused indefinitely until they are disconnected by the connected user.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCdu78087

  Symptoms: A “full” state may be displayed by the **show x25 hunt-group name** EXEC command for an interface participating in an X.25 hunt group when additional Virtual Circuits (VCs) are available. This symptom may cause all subsequent X.25 calls to use other interfaces that are participating in the hunt group.

  Conditions: This symptom may be observed when a Cisco router is configured for X.25 load balancing with hunt groups.

Workaround: There is no workaround.

- CSCdz25535

  Symptoms: The NAS-Port (Attribute 5) may become corrupted on a Cisco router.

  Conditions: This symptom is observed on a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) in a multihop environment.

  Workaround: There is no workaround.

- CSCdz31561

  Symptoms: A callback is initiated only once from a callback server when a dialer string is different from the calling number on a received call. Subsequent callback attempts are unsuccessful and may exhibit the following pattern:

```
: ISDN BR0: RX <- SETUP pd = 8 callref = 0x5A
: Bearer Capability i = 0x8890
: Channel ID i = 0x8A
: Calling Party Number i = 0x81, '1010', Plan:ISDN, Type:Unknown
: Called Party Number i = 0x81, '222', Plan:ISDN, Type:Unknown
: ISDN BR0: Event: Received a DATA call from 1010 on B2 at 64 Kb/s
: BR0:2 DDR: Caller id 1010 matched to profile
: Di1 DDR: callback to 1010 already started
: ISDN BR0: TX -> RELEASE_COMP pd = 8 callref = 0xDA
: Cause i = 0x8095 - Call rejected
```

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(17).

  Workaround: There is no workaround.

- CSCdz66576

  Symptoms: When large numbers of Layer 2 Tunneling Protocol (L2TP) sessions are dropped, "thrashing" occurs with the virtual private dialup network (VPDN) history manager.

  Conditions: This symptom is observed on L2TP access concentrators (LAC) when the tunnels are shut down.

  Workaround: There is no workaround.

- CSCdz80585

  Symptoms: A memory leak that is related to the establishment of a soft permanent virtual circuit (Soft-PVC) may occur on a Node Switch Processor (NSP) and may cause the NSP to reload. The output of the **show process memory** EXEC command displays that the following processes are holding increasingly more memory before the NSP reloads:

```
99 0 749976 188 495828 205200 0 SSCOP Output
100 0 779188 188 674656 213300 0 SSCOP Timer
104 0 73288716 56730436 537532 18000 0 ATMSIG CC
105 0 2018648 11308324 1495424 566208 0 ATMSIG Output
```

  After the NSP has reloaded, the output of the **show process memory** EXEC command displays the following information:

```
99 0 65976 188 58388 18000 0 SSCOP Output
100 0 13316 188 13400 3600 0 SSCOP Timer
104 0 5347324 4073920 279760 0 0 ATMSIG CC
105 0 241824 785352 126020 88704 0 ATMSIG Output
```

Conditions: The memory leak occurs slowly, and the memory loss will become significant after a day or more, eventually causing the NSP to reload.

Workaround: There is no workaround.

- CSCea19848

  Symptom: Multilink PPP (MLP) fragmentation drops may occur on a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS).

  Conditions: This symptom is observed when the maximum transmission unit (MTU) size that is negotiated is any size other than 1500 and Cisco Express Forwarding (CEF) is enabled.

  Workaround: Configure an MTU size of 1500 on both the client device and the LNS.

  Alternate Workaround: Disable CEF on the LNS.

- CSCea22898

  Symptoms: The value of the Logical Link Control (LLC) N2 error counter may not reset when no information frames (I-frames) are sent and acknowledged. When final Receive Ready frames are dropped, the error counter is increased, but when a proper final Receive Ready frame (in which the next received [nr] frame equals the next sent [ns] frame) is received, the error counter is not reset.

  Conditions: This symptom is observed when a Systems Network Architecture (SNA) LLC connection is made. Each side sends a single I-frame or no I-frame; then, the connection remains idle for many hours. Final Receive Ready packets are dropped in the network, causing the T1 timer to expire. When this situation occurs often, the value of the *retry-count* argument of the **llc2 n2** *retry-count* internal adapter configuration command may be exceeded, and the SNA connection may be terminated.

  Workaround: When the SNA LLC connection is slow, increase the T1 timer by entering the **llc2 t1-timer** *milliseconds* internal adapter configuration command.

  First Alternate Workaround: Increase the value of the *retry-count* argument of the **llc2 n2** *retry-count* internal adapter configuration command.

  Second Alternate Workaround: Ensure that I-frames continue to be sent in both directions.

- CSCea24708

  Symptoms: A valid X.25 call received in the appropriate one-way channel range (incoming-only for X.25 DTEs, outgoing-only for X.25 DCEs) may be refused by a Cisco router.

  Conditions: This symptom may occur when an X.25 interface is configured with one-way SVC ranges.

  Workaround: Extend the two-way channel range to include the offending one-way channel range.

- CSCea38851

  Symptoms: A router may reload with an address error exception.

  Conditions: This symptom is observed on a Cisco 7600 series router that is configured with Multilink PPP (MLP) on the serial links, and a reload on the peer router occurs.

  Workaround: There is no workaround.

- CSCea39282

  Symptoms: A Cisco 3600 series router that is configured for LAN Emulation (LANE) and bridging allows LANE Address Resolution Protocol (LE ARP) to be answered on a blocked port.

  Conditions: This symptom is observed on a Cisco 3600 series router that is running Cisco IOS Release 12.2 or Release 12.2 T.

  Workaround: There is no workaround.

- CSCea46367

  Symptoms: A Layer 2 Tunneling Protocol (L2TP) tunnel does not set up if the user logs on without the realm in the username (for example, user@domain.com where domain.com is the realm).

  Conditions: This symptom is observed on a Cisco AS5300 router that is running Cisco IOS Release 12.2(13b).

  Workaround: There is no workaround.

- CSCin08082

  Symptoms: A router may reload if the **no shutdown** interface configuration command is entered on a multilink interface or the **no multilink-group** interface configuration command is entered on a serial interface.

  Conditions: This symptom may occur if the **no multilink-group** interface configuration command is entered on a serial interface that is not configured for PPP encapsulation, or if PPP encapsulation is removed from a serial interface using the **no encapsulation ppp** interface configuration command if that interface is already configured as part of a multilink group.

  Workaround: Make sure that a serial interface is configured for PPP encapsulation using the **encapsulation ppp** interface configuration command before configuring a multilink group, and always make sure that the interface is not configured as part of a multilink group before removing PPP encapsulation.

Resolved Caveats—Cisco IOS Release 12.2(16f)

Cisco IOS Release 12.2(16f) is a rebuild release for Cisco IOS Release 12.2(16). The caveats in this section are resolved in Cisco IOS Release 12.2(16f) but may be open in previous Cisco IOS releases.

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.

IP Routing Protocols

- CSCed28873

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Miscellaneous

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Resolved Caveats—Cisco IOS Release 12.2(16c)

Cisco IOS Release 12.2(16c) is a rebuild release for Cisco IOS Release 12.2(16). The caveats in this section are resolved in Cisco IOS Release 12.2(16c) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCeb73681

  Symptoms: The main High-Speed Serial Interface (HSSI) interface flaps when you enter the **map-class frame-relay** global configuration command on a subinterface.

  Conditions: This symptom is observed only when map class contains both traffic shaping and Random Early Detection (RED).

  Workaround: Use only traffic shaping under the map-class.

Resolved Caveats—Cisco IOS Release 12.2(16b)

Cisco IOS Release 12.2(16b) is a rebuild release for Cisco IOS Release 12.2(16). The caveats in this section are resolved in Cisco IOS Release 12.2(16b) but may be open in previous Cisco IOS releases.

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.

Miscellaneous

- CSCdz88368

  Symptoms: A nonexistent policy map that is configured as the input or output service policy of an ATM virtual circuit (VC) causes a router to be unable to display or save its configuration.

Conditions: This symptom is observed on Cisco Route Processor Module (RPM) routers, but may affect any Cisco router that is using ATM interfaces.

Workaround: Do not specify nonexistent policy maps as an ATM VC service policy.

- CSCea55600

  Symptoms: A Frame Relay (FR) interface may go up and down continuously.

  Conditions: This symptom is observed on an FR interface when the keepalive timeout is set to one second and fragmentation and traffic shaping are enabled on multiple permanent virtual circuits (PVCs).

  Workaround: Increase the keepalive timeout to 5 seconds or more.

- CSCeb00104

  Symptoms: When configuration changes are made, a Cisco 7500 series Versatile Interface Processor (VIP) may pause indefinitely, produce large numbers of spurious memory accesses, or reload. This situation may cause the router to detect that interfaces on the VIP are not sending packets and to report that the output of the interfaces is stuck.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for fragmentation and shaping on a Frame Relay interface using modular QoS CLI (MQC).

  Workaround: Before you make quality of service (QoS) policy or Frame Relay fragmentation changes on an interface of the VIP, enter the shutdown interface configuration command on the interface.

- CSCeb02068

  Symptoms: In a configuration with multiple name servers, when one server times out, the other servers may not be contacted during name resolution.

  Conditions: This symptom is observed when the **ip domain-list** *name* global configuration command is enabled.

  Workaround: Replace the **ip domain-list** *name* global configuration command with the **ip domain-name** *name* global configuration command.

  Alternate Workaround: Explicitly specify a domain when resolving a name. For example, enter “anyname.cisco.com” instead of “anyname”.

Wide-Area Networking

- CSCea48995

  Symptom: The information element (IE) of a calling party number in an outgoing call setup message may be corrupted. When you use the Q.931 Translator, the log files may display that the calling party number in the outgoing call setup message is “0x00,” as in the following example:

```
ISDN Se0:23: TX -> SETUP pd = 8  callref = 0x0005
Bearer Capability i = 0x8890
Channel ID i = 0xA98397
Calling Party Number i = 0x00, (null),
Plan:Unknown, Type:Unknown
Calling Party SubAddr i = 0x80, '9876'
Called Party Number i = 0x80, '2222',
Plan:Unknown, Type:Unknown
```

  Condition: This symptom is observed after an IE for a calling party subaddress is received.

Workaround: There is no workaround.

- CSCea90880

  Symptoms: When you enter the **show frame-relay pvc** privileged EXEC command, a Cisco router may reload because of a bus error.

  Conditions: This symptom is observed when two users simultaneously edit the same data-link connection identifier (DLCI).

  Workaround: Ensure that only one person at a time edits a DLCI.

Resolved Caveats—Cisco IOS Release 12.2(16a)

Cisco IOS Release 12.2(16a) is a rebuild release for Cisco IOS Release 12.2(16). The caveats in this section are resolved in Cisco IOS Release 12.2(16a) but may be open in previous Cisco IOS releases.

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.

Basic System Services

- CSCdx04081

  Symptoms: A Cisco MC3810 router with a T1 controller may report line code violation (LCV) errors.

  Conditions: This symptom is observed on a Cisco MC3810 router with a T1 controller.

  Workaround: There is no workaround. The LCV errors are false errors and do not have an impact on the performance of the router. This symptom may be verified by using the **show controller t1** EXEC command.

- CSCdx07849

  Symptoms: An attempt to update the startup-config file using the **write memory** EXEC command may fail with the following error:

  ```
  startup-config file open failed (Device or resource busy)
  ```

  Conditions: This symptom may be caused by a process that is attempting to update NVRAM. To locate this process, use the **show file descriptors** EXEC command:

  ```
  Router# show file descriptors
  File Descriptors:
  FD Position Open PID Path
  0 0 430A 157 nvram:
  ```

  Use the **show process** EXEC command to find the process with the offending physical identification (PID). If the PID belongs to a process called “radius nvwrite,” this caveat may cause the symptom.

  Workaround: Save the current running configuration file to a temporary file in Flash memory or on a TFTP server. Reload the router. Immediately after reloading, copy the saved configuration to nvram:startup-config.

- CSCea15879

  Symptoms: A Cisco router that is configured with Cisco Service Assurance Agent (CSAA) may run out of memory and permanently pause because the round-trip home (RTT) responder process does not free memory.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13) and that is configured with CSAA.

  Workaround: Use the **no rtr responder** global configuration command followed by the **rtr responder** global configuration command.

IP Routing Protocols

- CSCdz46435

  Symptoms: A spurious memory access may occur, and a traceback may be generated when you deconfigure Protocol Independent Multicast (PIM).

  Conditions: This symptom is observed when you deconfigure PIM from a subinterface that is configured for Frame-Relay encapsulation.

  Workaround: There is no workaround.

Miscellaneous

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCdz85922

  Symptoms: A Cisco 7500 series router or a Cisco 12000 series Internet router may experience a reload of either the Versatile Interface Processor (VIP) or the line card and display the following message:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = TFIB Stats Background
  ```

  Conditions: These symptoms may affect only Cisco IOS releases with the fix for the caveat CSCdz32988 and only platforms that perform distributed Multiprotocol Label Switching (MPLS) forwarding. Cisco IOS releases that may contain these symptoms include Release 12.0(21)S, 12.0(22)S, 12.0(23)S, Release 12.1 and its derivatives, and Release 12.2 mainline. Cisco IOS Release 12.2 T and the latest Cisco IOS Release 12.0 S software are not susceptible to these symptoms.

  Workaround: There is no workaround.

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea24835

  Symptoms: A service policy that is attached to an interface without any priority feature and traffic is flowing through existing classes of that policy, stops traffic flowing through the other classes when adding the priority feature in that policy.

  Conditions: This symptom is observed when the interface that has the output service policy is congested when the priority feature is added to the policy map.

  Workaround: Remove and reattach the service policy to the interface.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea44554

  Symptoms: A Cisco gateway general packet radio service (GPRS) support node (GGSN) reloads with a bus error while updating fast cache.

  Conditions: This symptom is observed on a Cisco GGSN when fast switching is enabled and a “delete pdp (Protocol Data Packet) context” request is received.

  Workaround: There is no workaround.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Novell IPX, XNS, and Apollo Domain

- CSCdz18119

  Symptoms: A Cisco 3640 router may reload at "__doprnt."

Conditions: This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(13b) while the router is being configured for IPX routing.

Workaround: There is no workaround.

Wide-Area Networking

- CSCea24708

  Symptoms: A valid X.25 call received in the appropriate one-way channel range (incoming only for X.25 DTEs, outgoing only for X.25 DCEs) may be refused by a Cisco router.

  Conditions: This symptom may occur when an X.25 interface is configured with one-way switched virtual circuit (SVC) ranges.

  Workaround: Extend the two-way channel range to include the offending one-way channel range.

Resolved Caveats—Cisco IOS Release 12.2(16)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(16). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(16). This section describes severity 1 and 2 caveats and select severity 3 caveats.

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.

Basic System Services

- CSCdv36870

  Symptoms: The Compression Control Protocol (CCP) may restart on a router.

  Conditions: This symptom is observed on a Cisco 7500 series router that has fair queueing, distributed Cisco Express Forwarding (dCEF), and compression enabled on a serial interface.

  Workaround: Enter the **no fair-queue** command on the serial interface.

- CSCdw88209

  Symptoms: When a Cisco router is reloaded, the **rtr schedule** *operation* [**start-time** *hh:mm* [*month day*]] global configuration command is not loaded into the running configuration from NVRAM and the "The date and time must be set first" message is displayed even though the calendar and Network Time Protocol (NTP) have been set.

  Conditions: These symptoms have been observed on a Cisco router that is running Cisco Service Assurance Agent (SA Agent) when the collection time is being manually configured with the **rtr schedule** *operation* [**start-time** *hh:mm* [*month day*]] global configuration command.

  Workaround: There is no workaround.

- CSCdy54493

  Symptoms: A "%SNMP-3-CPUHOG: Processing GetNext of ciscoFlashDeviceEntry.5.8" error message is display during a Simple Network Management Protocol (SNMP) query on ciscoFlashDeviceEntry.

  Conditions: These symptoms can occur on any Cisco router that is running Cisco IOS software.

  Temporary Workaround: Exclude ciscoFlashMIB by entering the **snmp-server** global configuration command. If SNMP must be enabled on the Flash devices, then there is no workaround.

- CSCdy80552

  Symptoms: A memory leak in the ISDN process may cause a Cisco router that is operating under stress conditions to reload.

  Conditions: This symptom is observed when more than one host that uses the Simple Network Management Protocol version 1 (SNMPv1) security model is configured on the router by entering the **snmp-server host** *host-addr* global configuration command such as in the following configuration:

  ```
  snmp-server host 10.30.50.41
  snmp-server host 10.30.50.40
  ```

  Workaround: Remove the multiple instances of configured SNMPv1 hosts. Only one host should be specified in the running configuration by entering the **snmp-server host** *host-addr* global configuration command.

- CSCdz01381

  Symptoms: If a short and nonspecific dnis-number is specified in the **aaa dnis map** *dnis-number* **authorization network group** *server-group- name* global configuration command to map a dialed number identification service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group after a longer *dnis- number* (that shares the same first digits with the short nonspecific dnis-number) has been previously configured by entering the same command, the **aaa dnis map** *dnis-number* **authorization network group** *server-group- name* global configuration command that has the short and nonspecific *dnis-number* may not work as expected.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1, Release 12.2, or Release 12.2 T.

  Workaround: Enter the **aaa dnis map** *dnis- number* **authorization network group** *server-group-name* global configuration command that has the short and nonspecific *dnis-number* before entering the same command for the configuration that has the longer *dnis- number.*

- CSCdz22927

  Symptoms: PPP-Link Quality Monitoring (PPP-LQM) may fail to maintain link quality.

  Conditions: This symptom is observed when PPP-LQM is enabled with hardware compression (PA-COMP) on a Cisco 7200 series.

  Workaround: Disable hardware compression and use software compression when PPP-LQM is required.

- CSCdz31376

  Symptoms: A Versatile Interface Processor (VIP) reloads after the following sequence of commands is entered:

  – Enable distributed Cisco Express Forwarding (dCEF) by entering the **ip cef distributed** global configuration command.

  – Remove feature acceleration by entering the **no ip flow-cache feature-accelerate** global configuration command.

  - Configure Cisco Express Forwarding (CEF) by entering the **ip cef** global configuration command.
  - Enable dCEF by entering the **ip cef distributed** global configuration command.
  - Enable feature acceleration by entering the **ip flow-cache feature-accelerate** global configuration command.
  - Configure CEF by entering the **ip cef** global configuration command.

  Conditions: This symptom has been observed when NetFlow is configured on a subinterface and feature acceleration is configured.

  Workaround: There is no workaround other than to avoid this sequence of commands.

- CSCdz35713

  Symptoms: A Cisco router may reload upon configuration of ISDN-related commands. The router may also reload upon boot if ISDN commands are present in the startup configuration.

  The following error message may be seen:

  ```
  %SYS-2-STACK_OVERRUN: Stack of process 'ISDN' corrupted
  ```

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(23.3)S01, Release 12.2(13.4), or Release 12.2(13.4)T and occurs only with ISDN commands.

  Workaround: There is no workaround.

- CSCdz40567

  Symptoms: Counter overflow errors may be observed with the IP protocol on a serial interface.

  Conditions: This symptom is observed on the serial interface of a Cisco 7500 series.

  Workaround: There is no known workaround.

- CSCdz41092

  Symptoms: Alignment errors may occur on a Cisco 3600 series router because of spurious memory accesses. The output of the **show alignment** EXEC command displays the spurious memory accesses.

  Conditions: This symptom is observed on a Cisco 3600 series router that is running Cisco IOS Release 12.2(12a) when the **custom-queue- list** *list-number* interface configuration command is enabled on a BRI interface.

  Workaround: Disable fair queueing. Enter the following sequence of interface configuration commands on the BRI interface:

  no custom-queue-list *list-number*

  no fair-queue

  custom-queue-list *list-number*

- CSCdz49271

  Symptoms: A Cisco 3640 router may not receive Cisco Discovery Protocol (CDP) packets on its Fast Ethernet interface, preventing the router from recognizing its CDP neighbors. Outgoing CDP packets are sent without any difficulties, enabling other devices to recognize the Cisco 3640 router.

  Conditions: This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(12.14b).

  Workaround: There is no workaround. If possible, change to Cisco IOS Release 12.2(12b) in which the symptom does not occur.

- CSCdz51138

  Symptoms: An incorrect value is displayed for the ifOperStatus object for High-Speed Serial Interfaces (HSSIs) that are running PPP or propPointToPoint Serial encapsulation. A value of “6” (not present) is returned.

  Conditions: This symptom is observed when a Simple Network Management Protocol (SNMP) query is performed on the ifOperStatus object or the propPointToPointSerial encapsulation.

  Workaround: There is no workaround.

- CSCdz59003

  Symptoms: Frame Relay and ATM internetworking may not work as expected. Data may pass through, but discard eligibility/cell loss priority (DE/CLP) and explicit forward congestion indication/forward explicit congestion notification (EFCI/FECN) bit mapping may be mapped incorrectly. The DE bit is set to one when the CLP bit is zero from ATM to Frame Relay. The FECN bit is set to a value of 1 when the EFCI bit is zero from ATM to Frame Relay.

  Conditions: These symptoms are observed on a Cisco 3810 router that is running Cisco IOS Release 12.2(13)T.

  Workaround: There is no workaround.

  CSCin08377

  Symptoms: A Cisco router may reload upon setting and creating new entries in snmpTargetAddrTable. This operation is completed using Simple Network Management Protocol Version 3 (SNMPv3).

  Conditions: This symptom is observed on Cisco hardware.

  Workaround: There is no workaround.

- CSCin12235

  Symptoms: A waiting tty may not be removed from an asynchronous call queue for a rotary group.

  Conditions: This symptom is observed when the **clear line async-queue** EXEC command is entered.

  Workaround: There is no workaround.

IBM Connectivity

- CSCdy30993

  Symptoms: A router may reload.

  Conditions: This symptom is observed when the **stun route all** interface configuration command is configured on a serial tunnel (STUN) that already has a configured STUN route.

  Workaround: Remove the existing **stun route all** interface configuration command from the configuration and reenter the **stun route all** interface configuration command into the configuration.

- CSCdy36450

  Symptoms: Logical link control (LLC) circuits that are owned by an “active” data-link switching (DLSw) services Ethernet Redundancy (ER) router may be disconnected when service is restored on a failed DLSw ER router.

  Conditions: This symptom is observed in a failover scenario when DLSw ER is used on a router that is running Cisco IOS Release 12.2(10b). This symptom is observed only when the same MAC address is mapped to different Ethernet interfaces that are in different DLSw ER segments on two separate routers.

Workaround: Map both of the MAC addresses on the same router to different Ethernet interfaces.

Interfaces and Bridging

- CSCdt26857

  Symptoms: Asynchronous Transfer Mode (ATM) Adaptation Layer 5 (AAL5) packets and octet drop statistics are not supported with the Simple Network Management Protocol (SNMP).

  Conditions: There is no SNMP support to retrieve AAL5 packets and octet drop statistics on a Cisco 7200 series router. There is no Management Information Base (MIB) defined to provide support to retrieve AAL5 packets and octet drop statistics.

  Workaround: There is no workaround.

- CSCdt48893

  Symptoms: A Cisco router may pause indefinitely in rare traffic conditions.

  Conditions: This symptom is observed on a Cisco 7200 series router that is using an MPA-CE1 port adapter. This condition occurs if weighted fair queueing (WFQ) or Multilink PPP (MLP) is mixed with pure FIFO queueing on the configured channels.

  Workaround: There is no workaround.

- CSCdx39499

  Symptoms: A port adapter may stop receiving packets. When this symptom occurs, the output of the **show interface** EXEC command does not report any input or output drops. When the **show controller** EXEC command is issued on the Versatile Interface Processor (VIP) console of a router, the command output may display incrementing rx_no_buffer and virtual circuit connection (VCC) counts.

  Conditions: These symptoms are observed on the enhanced ATM Port Adapter (PA-A3) of a Cisco 7500 series.

  Workaround: Bounce the port adapter interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCdx63927

  Symptoms: A Cisco single-port Fast Ethernet 100BASE-TX port adaptor (PA-1FE) may cause a software-forced reload because of a block overrun.

  Conditions: This symptom has been observed on a Cisco 7200BR series router. Other Cisco series routers that use a PA-1FE may also exhibit this symptom. The symptom is a result of hitting a corner case. The likelihood of hitting a corner case increases with the number of interface resets.

  Workaround: There is no workaround.

- CSCdy61602

  Symptoms: X.25 does not function as expected on channelized T1 port adapter (PA-2CT1) and channelized E1 port adapter (PA-2CE1) interfaces.

  Conditions: This symptom is observed on Cisco 7500 series routers. In addition, messages such as “output frozen” and “not transmitting” may be seen on such interfaces. This may result in a CBUS complex.

  Workaround: There is no workaround.

- CSCdz73574

  Symptoms: On Cisco 7200 series routers, Super Frame (SF), Single Domain (SD), and Threshold Crossing Alarms B1, B2, and B3 (TCA_B1, TCA_B2, and TCA_B3) defects may not clear on a Packet-over-SONET (POS) port adapter (PA).

  When SF, SD, TCA_B1, TCA_B2, and TCA_B3 defects are asserted and de asserted very quickly on a POS PA on the router, the defects may not clear. This may cause the interface to pause permanently.

  Conditions: These symptoms are observed on Cisco 7200 series routers.

  Workaround: There is no workaround.

- CSCin16305

  Symptoms: Pings with packet sizes greater than 1496 bytes may fail

  Conditions: This symptom is observed on Ethernet 802.1Q subinterfaces.

  Workaround: There is no workaround.

- CSCin22287

  Symptoms: A router may permanently pause with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address-box crash
  ```

  Conditions: This symptom is observed on a Cisco router when there is active traffic on the subinterface and the VLAN encapsulation is changed.

  Workaround: Shut down the subinterface before changing the encapsulation, and then reload the subinterface after the encapsulation change is complete.

- CSCin24443

  Symptoms: On some T1 controllers, **no yellow generation** and **no yellow detection** are default configurations. In Cisco 7200 series and Cisco 7500 series, the default **no yellow <>** configuration will cause T1 controllers to stop detecting a yellow alarm and to stop generating a yellow alarm.

  Conditions: These symptoms are observed only on T1 controllers. These symptoms do not impact Cisco 2400 series, Cisco 2600 series, Cisco 3600 series, or the Cisco MC3810.

  Workaround: To configure a port adaptor (PA) for yellow alarm generation and detection, enter the following sequence of controller configuration commands:

  Router(config)# **controller T1**

  Router(config-controller)# **yellow generation**

  Router(config-controller)# **yellow detection**

  Router# **write**

- CSCin26599

  Symptoms: An A3 port adaptor (PA-A3) pauses, showing the rx_no_buffer counter increasing in the **show controller atm** output.

  Conditions: When high traffic is sent on a PA-A3, the PA may pause and stop receiving the traffic.

  Workaround: Use the **shutdown** and **no shutdown** EXEC commands on the interface.

- CSCin26892

  Symptoms: Input counters and rate counters may display a zero value.

  Conditions: This symptom is observed on a Cisco 7500 series that has an 8-port enhanced multichannel T1/E1 port adapter that has a channel service unit/data service unit (CSU/DSU) (PA-MC-8TE1+) or a PA-CE3 interface.

Workaround: Input counters may also be displayed by entering the **show interface serial stats** EXEC command. There is no alternative to display the input rate counters.

- CSCin27090

  Symptoms: A router permanently pauses with the following error message:
  `update_dot1q_vlan_rp_out_counters()`

  Conditions: This symptom is observed on a Cisco router when the VLAN encapsulation on the interface is changed with active traffic on the subinterface.

  Workaround: Shut down the subinterface before changing the encapsulation, and then reload the subinterface after the encapsulation change is complete.

IP Routing Protocols

- CSCdw75696

  Symptoms: Issuing the **clear ip mroute *** EXEC command under heavy multicast traffic, especially Internet Group Management Protocol (IGMP) traffic, may cause a watchdog timeout, and the router may permanently pause.

  Conditions: These symptoms are observed on Cisco 7500 series and Cisco 12000 series Internet routers that are running Cisco IOS releases prior to 12.0(22)S and 12.2(16).

  Workaround: There is no workaround.

- CSCdw82270

  Symptoms: If a Cisco 12000 series Internet router sends a **default-information originate** command via Border Gateway Protocol (BGP), the default route is learned correctly but entered incorrectly as "0.0.0.0/7" in the BGP routing table. This behavior may cause a problem in another router because that other router does not have a correct default route.

  The other issue is that if a default route is configured on this router and also other prefixes of the form 0.0.0.0/X with prefix length X in the range 1 to 32 and not including 0 (for example 0.0.0.0/20), then the default route does not work properly because the other 0.0.0.0/X routes might be chosen as the default route instead of 0.0.0.0/0. The default route 0.0.0.0/0 is not propagated in the BGP updates to the neighboring BGP peers.

  Conditions: This symptom is observed on a Cisco 12000 series Internet router.

  Workaround: Enter a static default route

  Alternate Workaround: Configure an access control list (ACL) to prevent the propagation from the "0.0.0.0/7" route:

  ```
  configure bgp route filtering
  neighbor 192.168.200.17 distribute-list 155 in
  access-list 155 deny ip host 0.0.0.0 host 254.0.0.0
  access-list 155 permit ip any any
  ```

- CSCdx95449

  Symptoms: When an Internet Group Management Protocol (IGMP) "receive" is issued on the incoming interface toward the Route Processor (RP), and a (source, group (S,G)) R state already exists for a source, the -R flag does not clear. The receiver does not receive traffic for that particular (source, group (S,G)) entry.

  Conditions: This symptom will cause the receiver to not receive traffic for this (source, group (S,G)) entry.

Workaround: Change the position of the RP to prevent this symptom from occurring.

- CSCdy24940

  Symptoms: A universal access server may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco AS5300 series universal access server that is running Cisco IOS Release 12.1(15).

  Workaround: There is no workaround.

- CSCdy29474

  Symptoms: Certain process such as the Standby process may be terminated when a HTTP packet is received on a router.

  Conditions: This symptom is observed on a Cisco 2600 series.

  Workaround: Disable the HTTP server process by entering the **no ip http server** global configuration command.

- CSCdy34931

  Symptoms: A Cisco router that is functioning as a Route Reflector (RR) may set itself as the Border Gateway Protocol (BGP) next hop while reflecting IP version 4 (IPv4) Virtual Private Network (VPNv4) routes to its internal BGP (iBGP) clients, even though the next hop configuration is not set toward its iBGP clients but toward the router itself.

  This situation mostly affects Multiprotocol Label Switching (MPLS) VPNs when the traffic path is not required to be through the RR, but does not affect IPv4 RRs when Cisco Express Forwarding (CEF) is enabled.

  Conditions: This symptom is observed in a BGP environment when the Cisco router that is functioning as the RR is running Cisco IOS Release 12.2(13)T1 or another release such as Release 12.2 M or Release 12.2 S and when peer groups are used for updates.

  Alternate workaround: Reset the BGP session either on the RR or on its clients.

- CSCdy59013

  Symptoms: When the **ip pim send-rp-announce** global configuration command is used, only the first entry in an access control list (ACL) table will switch to the new mode.

  Conditions: This symptom is observed on a Cisco router when a switch from bidirectional mode to sparse mode or from sparse mode to bidirectional mode occurs. The remaining entries in the ACL table remain in the earlier mode and do not switch.

  Workaround: Use the **clear ip pim rp mapping** EXEC command or the **no ip pim send-rp-announce** global configuration command before applying the new **ip pim send-rp-announce** command to change modes.

  Alternate workaround: Use the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command.

- CSCdy59996

  Symptoms: The Multicast Broader Gateway Protocol (MBGP) default route is advertised as 0.0.0.0/0 to a Protocol Independent Multicast (PIM) neighbor, but the MBGP default route is not considered for a multicast Reverse Path Forwarding (RPF) check on the router.

  Conditions: This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.2(10).

  Workaround: Use static routes, redistribution, or network statements by entering the **address-family ipv4 multicast** global configuration command.

- CSCdy60995

  Symptoms: When the **show ip pim rp mapping** EXEC command is executed, the router may reload.

  Conditions: This symptom is observed when Protocol Independent Multicast (PIM) Auto-Rendezvous Point (AutoRP) or bootstrap router (BSR) is configured on a router.

  Workaround: There is no workaround.

- CSCdy89663

  Symptoms: A Cisco 12000 series router may reload when an interface flaps.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(21)S during multicast traffic.

  Workaround: There is no workaround.

- CSCdz03337

  Symptoms: Traffic to downstream routers may be cut off.

  Conditions: This symptom is observed when a router has a bidirectional rendezvous point for a group range that covers a Source Specific Multicast (SSM) range when the router receives an SSM join message and it does not yet have the group state created. In this situation, the router rejects the SSM join message and causes traffic to downstream routers to be cut off.

  Workaround: There is no workaround.

- CSCdz04037

  Symptoms: A Cisco 3640 router reloads or permanently pauses with the following CPUHOG error messages on the console:

  ```
  %SYS-3-CPUHOG: Task ran for 3716 msec (147/54), process = IP NAT Ager, PC = 60420AB8.
  -Traceback= 60420AC0 609C1070 609C125C 609C1738 60405CEC 60405CD8 1d21h:
  %SYS-3-CPUHOG: Task ran for 3120 msec (133/68), process = IP NAT Ager, PC = 60420AB8.
  -Traceback= 60420AC0 609C1070 609C125C 609C1738 60405CEC 60405CD8 1d23h:
  %SYS-3-CPUHOG: Task ran for 2448 msec (76/49), process = IP NAT Ager, PC = 609C16F0.
  ```

  A stack trace points to ipnat_ager.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7c) or Release 12.2(12) when there are a large number of dynamic entries in the translation table.

  Workaround: There is no workaround.

- CSCdz08164

  Symptoms: A Cisco 7400 series router that is configured with Network Address Translation (NAT) experiences high CPU utilization.

  Conditions: This symptom is observed when a large number of TCP packet sessions are translated by the router and stay on the router for up to 24 hours even though the connections have been terminated.

  Workaround: Clear the translations table using the **clear ip nat translations** EXEC command.

- CSCdz08348

  Symptoms: The redistribution of unicast routes into Distance Vector Multicast Routing Protocol (DVMRP) may not function properly.

  Conditions: This symptom is observed when the **ip dvmrp metric** *metric* **list** *access-list-number* interface configuration command is executed. This command should allow all unicast routes that are allowed by the value of the *access-list-number* argument to be redistributed with the value of the *metric* argument, but only connected routes are advertised.

Workaround: Explicitly configure the unicast routing protocols that must be advertised, as in the following example:

ip dvmrp metric *metric* **list eigrp ip dvmrp metric** *metric* **list ospf**

- CSCdz09296

  Symptoms: Transit traffic that uses Open Shortest Path First (OSPF) routes may be briefly interrupted after consecutive switch-over. This affects only OSPF configurations with **message-digest** authentication.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 12.0(22)S when the following conditions are present:

  – The **message-digest** authentication is configured for OSPF.

  – More than one Route Processor (RP) switch-over occurs within minutes of each other.

  Workaround: There is no workaround. Traffic resumes without user intervention. To prevent future traffic interruptions on subsequent switch-overs, disable the **message-digest** authentication for OSPF.

- CSCdz12630

  Symptoms: Use of the **show ip ospf data *** EXEC command may cause a reload because of a bus error.

  Conditions: This symptom occurs when the **show ip ospf data *** EXEC command is used to display the contents of a malformed link-state advertisement (LSA) when the LSA is not a multiple of 4.

  Workaround: There is no workaround.

- CSCdz16276

  Symptoms: A router that is directly connected to a source may not start registering when the source becomes active, and the (S,G) state may time out on the route processor.

  Conditions: This symptom is observed on a router that is configured for Protocol Independent Multicast (PIM) and that has an (S,G) entry with the F flag reset.

  Workaround: There is no workaround.

- CSCdz24314

  Symptoms: An outbound route filter (ORF) may cause an incorrect “Open” message to be generated. This situation may bring a session down and generate a “Notification” message.

  Conditions: This symptom is observed in a Border Gateway Protocol (BGP) environment.

  Workaround: There is no workaround.

- CSCdz25073

  Symptoms: A software-forced reload may occur on a router.

  Conditions: This symptom is observed on a Cisco router when a register message is received.

  Workaround: There is no workaround.

- CSCdz25339

  Symptoms: An unusually formatted Multicast Source Discovery Protocol (MSDP) packet may cause a memory corruption to occur and a router to reload.

  Conditions: This symptom is observed on a Cisco router that has a peer relationship with a vendor router.

Workaround: If this symptom is observed on a Cisco router that has a peer relationship with vendor router, enter the **ip msdp shutdown** *peer-address* global configuration command to shut down the peer relationship with the vendor router.

- CSCdz26469

  Symptoms: Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors may be unnecessarily reset across an interface that is configured with summarization. This situation may be caused by the following "summary up, remove external" messages:

  ```
  %DUAL-5-NBRCHANGE: IP-EIGRP 111: Neighbor 10.108.255.244
  (FastEthernet4/0) is down: Summary up, remove external
  %DUAL-5-NBRCHANGE: IP-EIGRP 111: Neighbor 10.108.255.245
  (FastEthernet4/0) is down: Summary up, remove external
  %DUAL-5-NBRCHANGE: IP-EIGRP 111: Neighbor 10.108.255.244
  (FastEthernet4/0) is up: new adjacency
  %DUAL-5-NBRCHANGE: IP-EIGRP 111: Neighbor 10.108.255.245
  (FastEthernet4/0) is up: new adjacency
  ```

  Conditions: This symptom is observed when all components of a summary are lost and then at least one component is learned again, thereby triggering the summary to be regenerated.

  Workaround: Remove the EIGRP summary statements from the interface.

- CSCdz37639

  Symptoms: A Cisco router hangs up or permanently pauses to rommon.

  Conditions: This symptom is observed when stress reconfigurations, such as Protocol Independent Multicast (PIM) mode changes, adding or removing multicast-enabled interfaces, and clearing mroutes, result in many multicast routes being deleted and readded.

  Workaround: There is no workaround.

- CSCdz38773

  Symptoms: The **distribute-list 10 in ethernet 10** router configuration command may not be saved under a Virtual Private Network (VPN) routing/forwarding (VRF) instance.

  Conditions: The conditions under which this symptom is observed are unknown at this time.

  Workaround: Use the **distribute-list 10** router configuration command instead.

- CSCdz44155

  Symptoms: A Multilayer Switch Feature Card 2 (MSFC2) may create Network Address Translations (NATs) for which no expiration timer is set. These NAT entries will never time out.

  Conditions: This symptom is observed on an MSFC2 that is running Cisco IOS Release 12.1(13)E2 or Release 12.2(14)S and that has NAT configured.

  Workaround: There is no workaround. To remove the NAT entries, manually clear the NAT table.

- CSCdz45760

  Symptoms: A useless partial Shortest Path First (SPF) calculation may occur.

  Conditions: This symptom is observed when an Open Shortest Path First (OSPF) link-state advertisement (LSA) for a 0.0.0.0 destination is refreshed.

  Workaround: Use a static default route.

- CSCdz52552

  Symptoms: A software-forced reload may occur on a router.

Conditions: This symptom is observed on a Cisco router when a **no ip pim bidir-enable** is executed on the console window when another terminal window is displaying the output from **show ip pim interface df**

Workaround: There is no workaround.

- CSCdz58674

  Symptoms: When an area border router (ABR) receives type-4 link-state advertisements (LSAs) via the nonbackbone, the router may incorrectly generate type-4 LSAs into the backbone. This situation may cause a routing loop to occur.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(22)S or a later release or in Release 12.2(10) or a later release when the following conditions occur:

  – A router (referred to as Router 1) functions as an internal router in one particular area.
  – Router 1 has an inter-area route to an Autonomous System Boundary Router (ASBR) through the same area.
  – Router 1 is connected with another router (referred to as Router 2) in the backbone area, causing Router 1 to become an ABR.

  In this situation, Router 1 generates type-4 LSAs into the backbone area for the ASBR. This situation should not occur and may lead to a routing loop.

  Workaround: Reset the Open Shortest Path First (OSPF) process by entering the **clear ip ospf process** privileged EXEC command.

- CSCdz76611

  Symptoms: A router may reload when a static Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor statement is being removed.

  Conditions: If a static neighbor statement is removed from the EIGRP configuration at the same time the neighbor is going down, the router may reload.

  Workaround: Do not use static neighbors in EIGRP.

- CSCin31057

  Symptoms: A Cisco router may reload when a subinterface with a certain configuration is deleted.

  Conditions: This symptom is observed on a Cisco router that has multicast and the Hot Standby Router Protocol (HSRP) configured.

  Workaround: Remove the multicast configuration before deleting the subinterface.

- CSCuk38052

  Symptoms: The **neighbor** *ip-address* **capability** router configuration command or the **neighbor** *ip-address* **send-label** router configuration command cannot be configured.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12.10)T1.

  Workaround: There is no workaround.

Miscellaneous

- CSCdt23929

  Symptoms: A router may transmit bit errors.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1 and that has a serial 1DS3 or 2DS3 port adapter (PA-T3 or PA- 2T3) when the signal is below 0.5 decibels (dB).

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface.

- CSCdv33993

  Symptoms: An AS5400 may pause with a bus error exception during a stress test.

  Conditions: This symptom may occur during the execution of the **shutdown** and **no shutdown** interface command on the group async interface.

  Workaround: There is no workaround.

- CSCdv49909

  Symptoms: Parallel links may not be used efficiently on a Cisco router when Multiprotocol Label Switching (MPLS) traffic is load-balanced over parallel links to a customer premises equipment (CPE) device.

  Conditions: This symptom is observed when a Virtual Private Network (VPN) routing and forwarding (VRF) static route to a remote loopback interface is configured and both parallel links to the same CPE device are configured to the same loopback interface without an IP address using the **ip unnumbered** interface configuration command.

  Workaround: Define the following configurations on the provider edge (PE) and customer edge (CE) routers to achieve load balancing with static VRF routes:

  The PE configuration is as follows:

  ```
  interface multilink250
  ip vrf forwarding YELLOWVPN
  ip address 10.0.0.1 255.255.255.0
  interface multilink251
  ip vrf forwarding YELLOWVPN
  ip address 10.1.0.1 255.255.255.0
  ```

  The CE configuration is as follows:

  ```
  ip route vrf YELLOWVPN 10.10.0.1 255.255.255.255 10.0.0.2
  ip route vrf YELLOWVPN 10.10.0.1 255.255.255.255 10.1.0.2
  ```

  The following configuration defines static routes for the CE prefix:

  ```
  ip route vrf YELLOWVPN 192.168.200.0 255.255.255 0 10.10.0.1
  ```

  The links in the CE configuration must be configured with 10.0.0.2 and 10.1.0.2. 10.10.0.1/32 is the CE loopback and must be advertised to the PE via Routing Information Protocol (RIP) or via another router protocol. A static route may be used.

- CSCdv60884

  Symptoms: The Cable Dynamic Host Configuration Protocol (DHCP) proxy may cause registration difficulties at some sites.

  Conditions: This symptom is observed on a Cisco uBR905 router that is running Cisco IOS Release 12.2(2)T1 in routing mode and on a Cable Modem Termination System (CMTS) that is running Cisco IOS Release 12.0(14).

  Workaround: There is no workaround. Note that the symptom does not occur when the Cisco uBR905 router is running in bridging mode.

- CSCdw20927

  Symptoms: A Cisco AS5300 universal access server may reload and generate the following bus error:

  ```
  System was restarted by bus error at PC 0x6037BF80, address 0xD0D0D1D
  at Software (C5300-IS-M), Version 12.2(6), RELEASE SOFTWARE (fc2)
  Compiled Image text-base: 0x600089B0, data-base: 0x60F10000

  Stack trace from system failure: FP: 0x61B762C0, RA: 0x6037BF80 FP:
  0x61B762C0, RA: 0x6037A080 FP: 0x61B76308, RA: 0x6037A378 FP:
  0x61B76320, RA: 0x6037A47C FP: 0x61B76340, RA: 0x60E37C84 FP:
  0x61B76370, RA: 0x60E3C0D0 FP: 0x61B763B0, RA: 0x60DE8DB8 FP:
  0x61B763E8, RA: 0x60DE94A8
  ```

  Conditions: This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(6) and that is configured for interactive voice response (IVR).

  Workaround: There is no workaround.

- CSCdw31259

  Symptoms: An active FTP connection terminates after 30 seconds of transfer.

  Conditions: This symptom is observed on a Cisco 2600 series that is running a firewall image when the **ip inspect name** *inspection-name protocol* **timeout** *seconds* global configuration command is enabled and **ftp** is entered for the *protocol* argument. Passive FTP connections are not affected.

  Workaround: There is no workaround.

- CSCdw36564

  Symptoms: On a Cisco 3600 series router that is configured for Circuit Emulation Service (CES) with a 1-port ATM OC-3 Single mode long range network module (NM-1A-OC3SML-1V) and a 1-port E1 multi-flex voice/WAN interface card (VWIC-1MFT-E1), the CES circuit goes into Red alarm (Loss of Signal) and there is no way to recover.

  Conditions: This symptom is observed on a Cisco 3600 series that is configured for CES that is using revision B0 of the NM-1A-OC3SML. Revision A0 appears to function properly.

  Workaround: Use Revision A0 of the NM-1A-OC3SML.

- CSCdw68278

  Symptoms: Cisco IOS software allows the user to add variable bit rate real time (VBR-rt) permanent virtual circuits (PVCs) within a permanent virtual path (PVP).

  Conditions: This symptom is observed when a VBR-rt type of PVC is added within a PVP. Even though the command-line interface (CLI) permits this addition, the PVCs are converted back to an unspecified bit rate (UBR) type.

  Workaround: There is no workaround.

- CSCdw72560

  Symptoms: Different speeds cannot be set on a serial interface.

  Conditions: This symptom is observed when circuit emulation service (CES) is configured on a Cisco MC3810. Different speeds cannot be set on the serial 0 and serial 1 interfaces.

  Workaround: There is no workaround.

- CSCdw87695

  Symptoms: On a router, an unnumbered acknowledgement (UA) that is not put on the wire may occur.

  Conditions: This symptom is observed on a Cisco router that uses a static terminal endpoint identifier (TEI) to transfer X.25 over a D channel.

  Workaround: There is no workaround.

- CSCdw94563

  Symptoms: After a Virtual Private Network (VPN) Routing and Forwarding (VRF) table is removed from a VPN, traffic continues to leak into public network space. Packets that originate within the VPN are still forwarded to a now non-VPN interface.

  Conditions: This symptom is observed on Cisco routers.

  Workaround: There is no workaround.

- CSCdx18122

  Symptoms: A uBR900 series or a CVA120 series will stop forwarding traffic from customer premise equipment (CPE) to head-end.

  Conditions: This symptom is observed when the attribute “docsDevCpeIpMax” is set equal to n, where n is the number of CPEs behind the Compatibility Matrix (CM). This symptom occurs only when the modem is configured as a bridge.

  Workaround: Set the attribute “docsDevCpeIpMax” = –1”.

- CSCdx31265

  Symptoms: Dial FTP throughput on a downlink may degrade by 18 percent.

  Conditions: This symptom is observed on a NextPort asynchronous modem interface on a Cisco AS5400 universal access gateway. The degradation in the throughput occurs because the NextPort asynchronous modem interface sends out misformatted packets on the PPP dialup link and causes retransmissions to occur with TCP-based client applications.

  Workaround: There is no workaround.

- CSCdx74321

  Symptoms: A Cisco router may generate undesired local label advertisement for prefixes learned via the Border Gateway Protocol (BGP). This results in a traffic drop.

  Conditions: This symptom is observed when the route for the prefix is advertised by both BGP and Interior Gateway Protocol (IGP). When the BGP session goes down, the IGP route for the prefix takes over and Label Distribution Protocol (LDP) allocates and advertises the label for it. When the BGP session comes up, the LDP session withdraws the label after a 5-minute wait. Traffic is dropped until the label is withdrawn.

  Workaround: Use an access list to block local tags for the prefixes.

  Alternative workaround: Use the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command.

- CSCdx77062

  Symptoms: Following an Initial Program Load (IPL) of the host mainframes, a Systems Network Architecture Switching Services (SNASw) router displays Physical Units (PUs) in a reset state. (Using the **show snasw pu** EXEC command illustrates this.) Downstream devices in this state are unable to reconnect to this SNASw router.

  Conditions: This symptom is observed on a Cisco router that is configured with SNASw.

Workaround: Stop and then restart the SNASw subsystem.

- CSCdx77088

  Symptoms: A software-forced reload may occur on a router, and the following messages may be displayed:

  ```
  System was restarted by error - a Software forced crash, PC 0x60396E7C at 4500 Software
  (C4500-A3JS-M), Version 12.2(8.1), MAINTENANCE INTERIM SOFTWARE Compiled (current
  version) Image text-base: 0x60008948, data-base: 0x61116000 Stack trace from system
  failure: FP: 0x618A8458, RA: 0x60396E7C FP: 0x618A8458, RA: 0x603952F4 FP: 0x618A8480,
  RA: 0x6039D584 FP: 0x618A84A0, RA: 0x603A0CC8 FP: 0x618A84C0, RA: 0x60398BDC FP:
  0x618A8558, RA: 0x6037E1F0 FP: 0x618A85A0, RA: 0x6174B1F0
  ```

  Conditions: This symptom is observed on a Cisco 4500 router that is running Cisco IOS Release 12.2(8.1).

  Workaround: There is no workaround.

- CSCdx81839

  Symptoms: Routes from a remote customer edge (CE) router may not appear on another CE router.

  Alternatively, routes from a remote CE router may appear on another CE router, but the addresses from the remote CE router cannot be pinged. Virtual Private Network (VPN) routes between the CEs may be lost.

  Conditions: These symptoms are observed when the MPLS VPN Inter-ASóIPv4 BGP Label Distribution feature is enabled on two Multiprotocol Label Switching (MPLS) VPN autonomous systems that are separated by a non-MPLS VPN autonomous system, and when the interfaces on the autonomous system border routers (ASBRs) between the MPLS VPN autonomous systems and the non-MPLS VPN autonomous system are interfaces of 3-port Gigabit Ethernet line cards. The ASBR routers are Cisco 12406 routers that are running the gsr-p-mz image of Cisco IOS Release 12.0(22.1)S1.

  In the above-mentioned topology, if the **clear ip route *** EXEC command is entered on any of the ASBRs or CE routers, VPN routes between the CEs may be lost.

  Workaround: Do not enter the **clear ip route *** EXEC command on any of the ASBRs or CE routers.

  If it is necessary to enter the **clear ip route *** EXEC command, reload the ASBR router on each side of the Gigabit Ethernet link (that is, the ASBR at the side of the MPLS VPN autonomous system and the ASBR at the side of the non-MPLS VPN autonomous system).

  Note: Reloading a router may have a severe impact upon a network and its users, depending upon the topology and the time of day.

- CSCdx87631

  Symptoms: A Cisco gateway card may reload because the I/O memory is corrupted. The following output may be displayed when the **show version** EXEC command is entered after the Cisco gateway card reloads:

  ```
  System returned to ROM by error - a SIGTRAP exception, PC 0x802916DC
  ```

  Conditions: This symptom is observed on a Cisco gateway card that is running Cisco IOS Release 12.2(10a).

  Workaround: There is no workaround.

- CSCdx93111

  Symptoms: The hardware forwarding information base (HW FIB) points to an incorrect adjacency entry when a recursive lookup is involved.

  Conditions: This symptom is observed on a Cisco 6500 series.

Workaround: Use the **clear ip route *** EXEC command, and build the HW forwarding and adjacency tables again.

Specify an interface in the static route (if used for the dependent route) as follows:

```
ip route 10.10.10.10 255.255.255.0 FastEthernet3/1
```

- CSCdy06079

  Symptoms: A Cisco 7200 Network Service Engine 1 (NSE-1) or a Cisco 7401 router may reload after the **show ip cache flow** EXEC command is entered. Exported flow statistics may also be incorrect when this symptom occurs.

  Conditions: This symptom is observed when Parallel Express Forwarding (PXF) is enabled and is more likely to occur when many flows (more than 100,000) are active.

  Workaround: Disable PXF by entering the **no ip pxf** global configuration command.

- CSCdy07690

  Symptoms: An Access Gateway Module (AGM) blade fails to transcode a G.711 music on hold (MoH) stream to G.729. The packets are dropped instead of being transcoded. As the number of drop packets that the CPU has to process increases, a degradation of voice quality and the deregistration of the transcoder may be observed.

  Conditions: This symptom is observed on an AGM blade.

  Workaround: Disable MOH or enable G.729 or enable G.729 under IP voice streaming application service parameters.

- CSCdy09517

  Symptoms: Voice packets may assume the source address of a serial subinterface even after the **h323-gateway voip bind srcaddr** *ip_address* interface configuration command is configured on a different interface. This symptom is observed on the first call or the first set of calls after the router is reloaded. The second and subsequent calls work normally and have voice packets that have the correct source address.

  Conditions: This symptom is observed on a Cisco 2600 or 3600 router that is running Voice over IP (VoIP) over Frame Relay and quality of service (QoS).

  Workaround: Add a line to the VoIP access control list (ACL) to permit voice packets that have User Datagram Protocol (UDP) ports in the range of 16384 to 32767 and use the source address of the serial subinterface.

- CSCdy11913

  Symptoms: Cyclic redundancy check (CRC) input errors may be observed on an interface. This congestion may limit traffic performance on the router.

  Conditions: This symptom is observed on the ATM interface of a Cisco 6400 Node Route Processor (NRP) that is configured as a provider edge (PE) router. This symptom is observed in a RADIUS to Multiprotocol Label Switching (MPLS) or Virtual Private Network (VPN) environment in which traffic is sent from a MPLS or VPN network to end users.

  Workaround: There is no workaround.

- CSCdy20760

  Symptoms: A software-forced reload may be observed on a Cisco AS5300 universal access server. The following error message may be displayed when the **show version** EXEC command is entered:

  ```
  System returned to ROM by error - a Software forced crash,PC 0xXXXXXXXX "0xXXXXXXXX"
  represents the program counter on which the reload occurred.
  ```

Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.1(16).

Workaround: There is no workaround.

- CSCdy22201

  Symptoms: A Versatile Interface Processor (VIP) located on a Cisco Route Switch Processor (RSP) permanently pauses.

  Conditions: This symptom is observed on the VIP when the **clear ip mds forwarding** EXEC command is executed with debugging turned on.

  Workaround: There is no workaround.

- CSCdy24838

  Symptoms: Physical units remain in the Pend Activate Physical Unit (ACTPU) state, and the **show snasw pu** EXEC command shows several downstream physical units (DSPUs) that have the same IDBLK/IDNUM physical unit identifier. The virtual telecommunications access method (VTAM) may be slow to send a response to the Request Activate Physical Unit (REQACTPU), and the DSPU disconnects and reconnects before the response arrives from VTAM. When the DSPU reconnects, Systems Network Architecture (SNA) Switching Services (SNASw) may treat the DSPU as a new DSPU. When VTAM sends the REQACTPU, SNASw may assume that there are two DSPUs with the same name and rejects the request with a 082C 002 sense code.

  Conditions: This symptom is observed when the user is waiting for the REQACTPU from the VTAM.

  Workaround: There is no workaround.

- CSCdy24900

  Symptoms: A Cisco 3600 series may permanently pause with a bus error and display the following message on the console:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0xXX, pc=0xXXXXXXXX,
  ra=0xXXXXXXXX, sp=0xXXXXXXXX
  ```

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0xXX, pc=0xXXXXXXXX,
  ra=0xXXXXXXXX, sp=0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a Cisco 3600 series that is running Cisco IOS Release 12.2(10a).

  Workaround: There is no workaround.

- CSCdy27286

  Symptoms: When performing Policy-Based Routing (PBR) on a dialer interface, the PBR does not function properly when distributed Cisco Express Forwarding (dCEF) is globally enabled.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1 E.

  Workaround: There is no workaround.

- CSCdy30984

  Symptoms: Transmit and receive statistics counters may show inaccurate numbers for some interfaces.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no known workaround when compression is disabled on the interface. If compression is enabled on the interface, the **show compress** EXEC command can be entered to obtain transmit and receive statistics.

- CSCdy31164

  Symptoms: Cisco Express Forwarding (CEF) may become disabled on the Versatile Interface Processor (VIP) of the Route Switch Processor (RSP).

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(13)T.

  Workaround: Reload the line card or reload the Cisco 7500 series.

- CSCdy41378

  Symptoms: IP Security (IPSec) may fail to encrypt traffic when the hardware crypto accelerator is used and when Fast switching or Cisco Express Forwarding (CEF) switching is enabled. The hardware crypto accelerator may return the following error message:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption Error,
  Invalid Packet
  ```

  Conditions: This symptom is observed with almost all types of IPSec configurations. The symptom is prevalent when there is Layer 2 (L2) padding in the packet.

  Workaround: There is no workaround.

- CSCdy44209

  Symptoms: A memory leak may occur on a router when Multilink PPP (MLP) and legacy Random Early Detection (RED) processes hog the memory on the router. The following message is logged on the router when this symptom occurs:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 904 bytes failed from 0x60291478, pool
  Processor, alignment 0 -Process= "IP Input", ipl= 0, pid= 11 Traceback= 60201A54
  6020329C 60291480 602691B8 6025EF00 6025F6DC 6025E79C 6025E94C 6025EAA8 601FD588
  601FD574 ***
  ```

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10a).

  Workaround: Remove legacy RED and replace it with modular QoS CLI (MQC) Weighted Random Early Detection (WRED). For more information about memory allocation failures, please refer to the document titled "Troubleshooting Memory Problems" at the following URL:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- CSCdy48848

  Symptoms: A Versatile Interface Processor (VIP) may reload when Compressed Real-Time Protocol (cRTP) header compression is disabled on a Frame Relay interface.

  Conditions: This symptom is observed on the serial interface of a Cisco router when the **no frame-relay ip tcp header-compression** interface configuration command or the **no frame-relay ip rtp header-compression** interface configuration command is entered.

  Workaround: Ensure that the serial interface is shut down before cRTP header compression is disabled.

- CSCdy54385

  Symptoms: After a second switchover occurs, a Cisco 7200 series or Cisco 7500 series router that is functioning as a backup router becomes active and the primary router goes into standby mode, but the Cisco 7200 series or Cisco 7500 series router may fail to handle connections that are directed at its virtual Hot Standby Router Protocol (HSRP) address and may not respond to pings that are directed at its HSRP address at the client side, server side, or both.

Conditions: These symptoms are observed when you use a Cisco Catalyst 6000 series switch as the primary router and a Cisco 7200 series or Cisco 7500 series router as a backup router that is configured with a 2-port Fast Ethernet/Inter-Switch Link (ISL) port adapter (PA-2FEISL) that has at least one Fast Ethernet interface configured for HSRP, and when a second switchover occurs. The symptom occurs only with Fast Ethernet interfaces of a specific third-party vendor.

The symptoms occur because the Fast Ethernet interface that is configured for HSRP is not switched to promiscuous mode when the HSRP group becomes active for the second time, preventing packets that are addressed to the HSRP virtual MAC address from being received by the interface. The output of the **show controllers fastethernet** EXEC command displays whether the promiscuous mode is enabled or disabled.

Reboot the Cisco 7200 series or Cisco 7500 series router to restore the router to proper backup operation.

Workaround: Enable the **standby use-bia** interface configuration command on the HSRP interface.

- CSCdy62448

  Symptoms: A PA-8T1 IMA port adapter will stop forwarding traffic over one or more of the T1 interfaces. There will be an increasing number of "output queue drops" reported by a **show interface atm** [*x/y*] EXEC command. The "output queue" will equal "40/40" in the output received after executing the **show queueing interface atm** [*x/y*] EXEC command.

  Conditions: These symptoms have been observed on a PA-8T1 IMA port adapter installed in a Cisco 7200 series router.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command under the (config-if)# prompt of the main ATM interface "<x/y>". The symptoms will clear for an undetermined time period.

- CSCdy64225

  Symptoms: A 2-port serial WAN interface card (WIC-2T) may stop receiving traffic for 50 seconds and may eventually reload because of missed keepalives.

  Conditions: These symptoms are observed on the WIC-2T interface of a Cisco 3640 that is running Cisco IOS Release 12.2(11)T. These symptoms occur after a large burst of traffic overruns the interface.

  Workaround: Disable fast switching, increase the keepalive interval, or find the source of the traffic that causes this issue and filter the traffic that is originating from the source.

- CSCdy67728

  Symptoms: A Versatile Interface Processor 2 (VIP2) card may reload after a redundancy-forced switchover. The reload may be observed immediately when the new primary VIP card activates the interfaces after a switchover occurs or when the old primary VIP card boots up.

  Conditions: This symptom is observed on the VIP2 card of a Cisco 7500 series that has Route Processor Redundancy Plus (RPR+) and Multiprotocol Label Switching (MPLS) configured. When an MPLS packet arrives on the VIP interface while Cisco Extended Bus (CyBus) is restarting, the VIP may drop all incoming MPLS packets.

  This symptom affects VIP modules and other modules such as the Gigabit Ethernet Interface Processor (GEIP).

  Workaround: There is no workaround.

- CSCdy68457

  Symptoms: Spurious memory accesses may occur on a Cisco router and cause it to reload.

  Conditions: This symptom is observed on a Cisco router that is configured for authentication proxy.

Workaround: There is no workaround.

- CSCdy68922

  Symptoms: A software condition may cause a router to reload, and a "%SYS-3- OVERRUN" error message may be generated.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(12) and that is configured for NetFlow and Parallel Express Forwarding (PXF). The symptom is more likely to occur during periods of congestion.

  Workaround: Disable PXF.

- CSCdy68935

  Symptoms: Voice calls that use a Virtual Private Network (VPN) card may not work with some IP Security (IPSec) transforms.

  Conditions: This symptom is observed on a Cisco router that has a voice or digital signal processor (DSP) module (NM-HDV, NM-HDA, NM-1V/2V, AIM-ATM-VOICE30, AIM-VOICE-30) and that uses a VPN card (AIM-VPN/BP, NM- VPN/MP, AIM-VPN/HP, AIM-VPN/EP) to encrypt voice calls. The use of authentication header (AH) transform options with Encapsulating Security Payload (ESP) encryption may result in poor voice quality.

  Workaround: Disable hardware encryption or configure a transform set without an AH transform option.

- CSCdy70210

  Symptoms: An R2 interface cannot send a release-ack signal to a PBX.

  Conditions: This symptom is observed on a Cisco 2611 router that is running Cisco IOS image c2600-is-mz.122-11.T.bin.

  Workaround: There is no workaround.

- CSCdy72994

  Symptoms: When the cable interface on a cable modem that is configured for routing is reset, the cable modem may lose IP connectivity between the ethernet interface and the connected device. Both the cable interface and Ethernet interface will be reachable via IP through the cable interface.

  When this symptom occurs, Address Resolution Protocol (ARP) entries in the cable modem for the LAN segment and the Ethernet interface will remain in the "up/up" state. The network that is on the Ethernet interface on the routing table will remain and routing information is passed from the cable modem to the Cable Modem Termination System (CMTS).

  Conditions: This symptom is observed on a Cisco uBR905 router or Cisco uBR925 router that is running Cisco IOS Release 12.2(8)T5.

  Workaround: Clear the IP routing table.

- CSCdy74807

  Symptoms: NetBios connections may not complete.

  Conditions: This symptom is observed when a port channel is configured and a bridge group is coded for data-link switching (DLSw) on the port channel.

  Workaround: Remove the port channel from the interface.

- CSCdy76759

  Symptoms: A 2-port Fast Ethernet port adapter (PA-2FE) may stop sending packets.

  Conditions: This symptom is observed only when there is a heavy traffic load on the PA-2FE port adapter of a Cisco router.

Workaround: There is no workaround.

- CSCdy79517

  Symptoms: A router permanently pauses in response to a user command that causes the router to switch from hardware crypto mode to software crypto mode while tunnels are actively being removed.

  Conditions: This symptom is observed on a Route Processor (RP) that is configured with a large number of Internet Key Exchange (IKE) tunnels and IP Security (IPSec) tunnels.

  Workaround: Remove all IKE and IPsecs before switching to software crypto mode. This can be accomplished by using the **clear crypto ipsec sa** and **clear crypto isakmp sa** global configuration commands and then verifying that all tunnels are down using the **show crypto eli** EXEC command. New tunnels should be prevented from starting, perhaps by shutting down the associated interfaces.

- CSCdy81201

  Symptoms: A ping may go through for the first five packets, but a subsequent ping may cause a router to reload.

  Conditions: This symptom is observed when a ping is issued on a permanent virtual circuit (PVC) over a BRI interface that is running hardware Frame Relay Payload Compression (FRF.9).

  Workaround: There is no workaround.

- CSCdy81947

  Symptoms: When debug traces are logged to a memory buffer, some debug messages may be missing from the trace, making it difficult to diagnose system problems.

  Conditions: This symptom is observed when there is a heavy traffic load.

  Workaround: There is no workaround.

- CSCdy84285

  Symptoms: When a client receives a specific address (for example, x.x.x.x) through the Dynamic Host Configuration Protocol (DHCP) unnumbered relay, a static route is added for x.x.x.x by the relay. When the same client reboots or when some other client attempts to acquire the same address, the DHCP relay fails to broadcast the DHCPACK response back to the client. Instead, the DHCP relay sends an Address Resolution Protocol (ARP) request for this address. Because of this behavior, the client is not able to acquire the x.x.x.x address.

  Conditions: This symptom is observed only when the route already exists on the DHCP relay.

  Workaround: Enter the **clear ip route dhcp** *destination gateway* privileged EXEC command to delete IP routing table entries. The *destination gateway* variable should be substituted with the x.x.x.x address.

- CSCdy84855

  Symptoms: An R2 timer may expire after waiting for 15 seconds for a remote “alerting” message, causing a call to fail.

  Conditions: This symptom is observed on a Cisco 3660 router when a PSTN-to- VoIP-to-PSTN call is made via a gateway that uses R2 signaling and via a terminating gateway that uses ISDN signaling and when the Public Switched Telephone Network (PSTN) network behind the terminating gateway has a number of legacy switches that use multiple analog trunks, causing delays up to 60 seconds.

  R2 signaling on the gateway expects an “alerting” message on the outgoing Voice over IP (VoIP) call leg and waits for a period of 15 seconds. If the “alerting” message is received, the gateway sends a “B6” message to the originating voice port. If no “alerting” message is received within 15 seconds, the gateway sends an “A4” message, indicating that there is congestion.

Workaround: There is no workaround.

- CSCdz00425

  Symptoms: An IP routing table may enter an inconsistent state (the same route may be shown as connected and redistribute connected) because of a PA-2FE interface flap. This occurs when the PA-2FE interface's network is added in any routing protocol

  Conditions: This symptom is observed on Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

- CSCdz04423

  Symptoms: CPU hog messages may be displayed on a router. The router may reload if heavy traffic is present while the router is booting up.

  Conditions: In Cisco IOS releases that contain the Network-Based Application Recognition (NBAR) resource manager, the "stile_expand_links()" causes a CPU hog traceback on low-end platforms when loading a Packet Description Language Module (PDLM) file and on high-end platforms when bursty traffic occurs.

  Workaround: There is no workaround.

- CSCdz05404

  Symptoms: After the serial interface is reset, any attempt to make outgoing ISDN asynchronous calls fails because the B channel is not available.

  Conditions: This symptom is observed on outgoing calls after the **shutdown** and **no shutdown** EXEC commands are executed on the D channel interface.

  Workaround: There is no workaround.

- CSCdz08017

  Symptoms: Digital signal processors (DSPs) are not released after a call is made, and the ports are stuck in the "dormant" state. All subsequent outbound calls that are placed through the port will fail.

  Conditions: This symptom is observed on the ports of a 2-port Foreign Exchange Office (FXO) voice interface card (VIC-2FXO) on a Cisco VG200 that is running Cisco IOS Release 12.2(11)T1.

  Workaround: Enter the **csim start** command on the port after the port is restored or enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port.

- CSCdz08278

  Symptoms: When receiving the atmIntfPvcFailuresTrap notification, ifIndex is given as an index to the subinterface of the failing ATM permanent virtual circuit (PVC). There is no direct method to determine the virtual path identifier (VPI) and virtual channel identifier (VCI) of the failing PVC.

  Conditions: This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.1(5).

  Workaround: Issue a Simple Network Management Protocol (SNMP) query on the atmCurrentlyFailingPVclTable to determine the failing PVC.

- CSCdz09542

  Symptoms: A High-Speed Serial Interface (HSSI) may stop transmitting traffic for some time and then recover. When the HSSI stops transmitting traffic, the output of the show interfaces privileged EXEC command displays the following message: "Output queue 40/40."

  Conditions: This symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCdz10165

  Symptoms: The Tag Forwarding Information Base (TFIB) entry for a Virtual Private Network (VPN) routing and forwarding (VRF) static recursive route that has Border Gateway Protocol (BGP) multipath may be lost.

  Conditions: This symptom is observed after an outgoing interface is flapped.

  Workaround: There is no workaround.

- CSCdz10787

  Symptoms: When a label switching router (LSR) reroutes some destinations and selects another interface, the upstream LSR for these destinations may lose the headend label bindings for them.

  Conditions: This symptom is observed in a Multiprotocol Label Switching (MPLS) ATM network when Intermediate System-to-Intermediate System (IS-IS) is used as the routing protocol.

  Temporary Workaround: Enter the **clear ip route** *network* EXEC command for the affected destinations until the symptom occurs again.

- CSCdz12098

  Symptoms: When auth-proxy is enabled in an environment where DOS attacks from CodeRed or Nimda are present, it may be possible to exhaust resources.

  Conditions: This symptom is observed where more than 40 DOS machines are attacking the router where auth-proxy is enabled.

  Workaround: Disable auth-proxy or monitor auth-proxy cache to see the attacking machines and clear viruses off the machines.

- CSCdz12429

  Symptoms: A large number of error messages may cause the logger queue to be filled up. The system may pause indefinitely as console messages cannot be rate limited.

  Conditions: This symptom is observed when logging rate-limit console global configuration command is configured.

  Workaround: There is no workaround.

- CSCdz15364

  Symptoms: Packets may not be passed when IP Cisco Express Forwarding (CEF) switching is configured with hardware encryption.

  Conditions: This symptom is observed on a Cisco 3600 series router.

  Workaround: Disable hardware encryption, and enable IP CEF switching.

  Alternate Workaround: Disable IP CEF switching, use fast switching instead, and enable hardware encryption.

- CSCdz15598

  Symptoms: Multiple codecs specified in Voice over IP (VoIP) dial peers, including g723r63 or g726r32, cause several dial peers to rotate with the same destination. The wrong 20-byte payload size is sent to the digital signal processor (DSP) which may cause the DSP to reload intermittently because g723r63 is expecting no less than a 24-byte payload, and g726r32 is expecting no less than a 40-byte payload.

  Conditions: This symptom is observed in a Cisco H.323 VoIP network and Media Gateway Control Protocol (MGCP) VoIP network.

  Workaround: There is no workaround.

- CSCdz15937

  Symptoms: Border Gateway Protocol (BGP) may install Tag Forwarding Information Base-Virtual Private Network version 4 (TFIB-VPNv4) entries for some prefixes without any change in the incoming or outgoing tags for the prefix.

  Conditions: This symptom is observed on an Autonomous System Border Router (ASBR) router that is performing VPNv4 label exchange.

  Workaround: There is no workaround

- CSCdz16552

  Symptoms: A Cisco 7200 series router may permanently pause during the online insertion and removal (OIR) of an integrated service adapter (ISA) crypto engine.

  Conditions: This symptom is observed on Cisco 7200 series routers if the rsa-sig or rsa-encr authentication method is used.

  Workaround: There is no workaround.

- CSCdz17156

  Symptoms: This caveat relates to two issues that are observed with two-stage calls.

  a. The second number is disconnected by a router if a dial peer is not found (with an unallocated number cause code). The PBX on the originating leg of the call then sends a disconnect with progress indicator (PI) signal. After the disconnect with PI signal is sent, the router does not send an ISDN release message as expected. Instead, the router waits 30 seconds for the ISDN T306 timer to expire.

  b. The originator disconnects after the second-stage call receives the alerting message. The call is not released for 30 seconds while the router waits 30 seconds for the ISDN T306 timer to expire.

  Workaround: There is no workaround, but the call will be released after 30 seconds.

- CSCdz17963

  Symptoms: A Cisco 2600 series or Cisco 3600 series router that is configured with a Multiflex Trunk (MFT) voice/WAN interface card (VWIC) that is installed in a Fast Ethernet (FE) combo network module (NM) may lose connectivity on port 0 of the MFT VWIC in slot 1 of the FE combo NM. This symptom does not occur on slot 0 of the FE combo NM.

  Conditions: This symptom is observed on a Cisco 2600 series or Cisco 3600 series router that is running Cisco IOS Release 12.2(12.4)T or a later release.

  Workaround: There is no workaround.

- CSCdz18424

  Symptoms: When the same policy map is attached to both the input and output direction of the same interface, applying a queueing feature to that policy map may permanently pause the router.

  Conditions: This symptom is observed on a Cisco router.

  Workaround: Do not apply queueing features to the policy map that is attached to the input direction.

- CSCdz18904

  Symptoms: The Cisco DistributedDirector may reboot and the following error message may be displayed if the “server verify-url” test is configured using the **ip director server verify-url *** global configuration command:

  ```
  %SYS-3-TIMERNEG
  ```

  Conditions: This symptom is observed if the user unconfigures or reconfigures the **ip director server verify-url** command.

Workaround: There is no workaround.

- CSCdz19278

  Symptoms: When an Internetwork Packet Exchange (IPX) access control list (ACL) is used as a classification criteria in a modular QoS CLI (MQC), the modification of the IPX ACL is not noted in the classification (a change on the IPX ACL does not affect classification).

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(16) and that has an IPX ACL-based QoS configuration.

  Workaround: Remove the class-map configuration of the IPX ACL before modifying the ACL. Construct a new class map under the IPX ACL after the IPX ACL is redefined.

- CSCdz19927

  Symptoms: When Flash memory wears out, some sectors may not fully erase and bad sectors are created. If a spare sector is not available to replace the bad one, the squeeze operation fails with an error.

  Conditions: This symptom is observed in all Cisco IOS releases.

  Workaround: Format the Flash memory with the spare sector option.

- CSCdz21534

  Symptoms: A T1 in a channelized T3 port (CT3) dial feature card (DFC) goes into a loopback. This can cause the remote to receive Path Code Violations (PCVs) and sometimes LoS (Loss of Signal).

  Conditions: This symptom is observed on a CT3 DFC on a Cisco AS5400 router.

  Workaround: Cable a hard loop to test from the network to the T3 of the Cisco AS5400.

- CSCdz21807

  Symptoms: A Cisco 2600 series router or a Cisco 3640 router that is using a T1 high-density voice network module (NM-HDV) for data (using a channel group configuration) and the compressed Real-Time Protocol (cRTP) will pass uncompressed RTP frames to the WAN when fast switching or Cisco Express Forwarding (CEF) switching is enabled on the T1 NM-HDV network module. This symptom does not occur if the Real-Time Transport Protocol (RTP) stream is generated by the router.

  Conditions: This symptom is observed on a Cisco 2600 series router or a Cisco 3640 router that has a T1 NM-HDV network module that is running Cisco IOS Release 12.2(8)T5, 12.2(11)T1, or Release 12.2(12.14)T1.

  Workaround: Configure the router to perform process switching on the WAN interface by entering the **no ip route-cache** interface configuration command. Verify the condition of the router before entering this command as the configuration of this command may increase the level of CPU processing on the router.

- CSCdz21952

  Symptoms: Upstream control point-to-control point (CP-CP) sessions may flap and very high CPU utilization may occur on a Systems Network Architecture switching services (SNASw) router.

  Conditions: This symptom is observed when two servers of a specific third- party vendor have the same logical unit (LU) name for a specific software application of the same third-party vendor. The symptom does not occur when other servers or other applications are used.

  The SNASw router registers the LU under the first server. When the second server comes up, it sends a registry message to the SNASw router, specifying resource type end node control point (ENCP). The SNASw router replies with sense code 0x08890000 (LU-to-LU session sense code 0x1014023C). The second server then sends a second registry message to the SNASw router without including the duplicate LU name, but specifying in the resource type in control vector 3C that it is

the network node control point (NNCP). Because the SNASw router does not expect a network node (NN) downstream, this second registry message causes the SNASw router to send an incorrect registry message to a virtual telecommunications access method (VTAM). The VTAM replies with sense code 0x08890100 and unbinds the CP-CP session.

The SNASw router then sends the incorrect registry message again, causing the CP-CP session to unbind again. This situation will repeat itself over and over again, causing very high CPU utilization in the SNASw router.

Reloading the SNASw router alleviates the situation, but only until the second server comes up again.

Workaround: There is no workaround. The duplicate LU name needs to be corrected in the servers of the third-party vendor.

- CSCdz25898

  Symptoms: As a dependent logical unit requester (DLUR), a Systems Network Architecture Switching Services (SNASw) switch must report all links to upstream nodes (end nodes or network nodes) in the initial topology database update (TDU) that it sends to the dependent logical unit sender (DLUS). Currently, the SNASw switch reports only uplinks to network nodes (NNs) and links to virtual routing nodes (VRNs). Links to upstream end nodes (ENs) must be included.

  Conditions: This symptom is observed on an SNAw switch that is running Cisco IOS Release 12.2 T.

  Workaround: Topology updates other than the initial TDU include ENs. Therefore, the link can be bounced to the EN to cause the DLUS to learn about the link after the initial topology has been reported.

- CSCdz28475

  Symptoms: The **ds0-group** *channel* **timeslots** *range type* signal controller configuration command cannot be configured with 15 channels on an E1 controller interface. This limitation allows only 30 channels to be configured on an E1 controller interface.

  Conditions: This symptom is observed on the E1 controller interface of a Cisco router that is running Cisco IOS Release 12.2(13)T.

  Workaround: There is no workaround.

- CSCdz30139

  Symptoms: Unexpected IP flow entries may be observed on a Cisco 7200 series that is running Parallel Express Forwarding (PXF). Packets that are either punted or dropped by PXF are counted in the flow statistics instead of being ignored.

  Conditions: This symptom is observed after the **ip route-cache flow** interface configuration command is configured on an interface.

  Workaround: Disable PXF by entering the **no ip route-cache flow** interface configuration command.

- CSCdz30655

  Symptoms: When a router attempts to send a “B6” message to a Telco side, the message may never be sent.

  Conditions: This symptom is observed on a Cisco 3600 series router when there is an attempt to hairpin a call from R2 to ISDN.

  Workaround: There is no workaround.

- CSCdz30790

  Symptoms: On a Cisco AS5400 router, Simple Network Management Protocol (SNMP) linkchange traps are not generated for a T3 controller up and down state changes.

  Conditions: This symptom is observed on a Cisco AS5400 router that is running a c5400-is-mz.122-2.XB9 image of Cisco IOS software and that is configured with the following router configuration command.

  snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

  Workaround: There is no workaround.

- CSCdz31314

  Symptoms: A 2-port Fast Ethernet port adapter (PA-2FE) that is used on a Cisco 7200 series router or on the Versatile Interface Processor (VIP) of a Cisco 7500 series router may become stuck. This symptom may also be observed on a Fast Ethernet interface that is used on the Cisco 7200 series 2-port 10/100 auto-sensing Fast Ethernet input/output controller (C7200-I/O-2FE/E).

  When the PA-2FE port adapter is used on the VIP of a Cisco 7500 series router, the VIP may reload unexpectedly and display the following output when the **show controllers vip** *slot-number* **logging** EXEC command is entered:

  ```
  00:34:32: RX FIFO was stuck - forced to reset MAC 00:34:34: RX FIFO was stuck - forced
  to reset MAC 00:34:37: RX FIFO was stuck - forced to reset MAC 00:34:43:
  %VIP-3-MVIP_CYBUSERROR_INTERRUPT: A Cybus Error occurred. 00:34:44:

  CYASIC Error Interrupt register 0x2000000 DMA Receive Error CYASIC Other Interrupt
  register 0x0 CYBUS Error Cmd/Addr 0x763AD80, CYBUS Error Data 0x0 MPUIntfc/PacketBus
  Error register 0x0
  ```

  When these symptoms occur, “RX FIFO was stuck - forced to reset MAC” log messages may be observed on a Cisco 7200 series router and in the log messages on the VIP of a Cisco 7500 series router.

  Conditions: These symptoms are observed when Inter-Switch Link (ISL) and Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) are used on a PA-2FE port adapter or when a Fast Ethernet interface is used on the C7200-I/O-2FE/E controller when there is a high traffic rate.

  Workaround: There is no workaround.

- CSCdz31682

  Symptoms: Packet drops may occur in the Cisco Express Forwarding (CEF) and distributed Cisco Express Forwarding (dCEF) paths after a router has been reloaded and a ping is sent (through the router) to the IP address of a directly connected customer edge (CE) router.

  Conditions: This symptom is observed on a Cisco 7500 series router. The CE router in this configuration is connected to a Fast Ethernet Virtual Private Network (VPN) routing/forwarding (VRF) dot1q subinterface on a provider edge (PE) router that has the **mpls netflow egress** interface configuration command enabled.

  Workaround: On the PE router, manually ping the IP address of the directly connected CE router and enable the relevant Address Resolution Protocol (ARP) entries to be populated.

  First Alternate Workaround: Disable the **mpls netflow egress** interface configuration command on the subinterface.

  Second Alternate Workaround: Add a static ARP entry for the VRF subinterface by entering the **arp vrf ip mask mac arpa** global configuration command.

  Third Alternate Workaround: Enter the **clear arp** privileged EXEC command on the destination CE router.

- CSCdz32940

  Symptoms: A Cisco router may reload unexpectedly when saving the configuration to NVRAM.

  Conditions: This symptom is observed on a Cisco router that is configured with the **service compress-config** global configuration command.

  Workaround: Enter the **no service compress-config** global configuration command.

  Alternate workaround: Use the **boot config** *filename* **nvbypass** global configuration command.

- CSCdz33759

  Symptoms: A Cisco router will permanently pause when a Frame Relay committed information rate (CIR) is being configured.

  Conditions: This symptom is observed if a very small value is given for the Frame Relay CIR.

  Workaround: There is no workaround.

- CSCdz34482

  Symptoms: The "camp-on" feature does not function correctly in an ISDN Voice over IP (VoIP) network.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 12.2(12.4)T.

  Workaround: Use Cisco IOS Release 12.2(8)T4.

- CSCdz35216

  Symptoms: A router permanently pauses when removing certain types of policies from the interface.

  Conditions: This symptom is observed on a Cisco router if the policy has bandwidth configured on class-default. When this policy is removed, the router permanently pauses.

  Workaround: There is no workaround.

- CSCdz35882

  Symptoms: More than 128 interfaces may fail to come up on an enhanced 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+). The 129th channel will fail to come up, and the following message may be displayed:

  ```
  %MCX-1-STARTFAIL: Serial1/0:27 channel not enabled
  ```

  Conditions: This symptom is observed when 128 interfaces are configured on a PA-MC-8TE1+ port adapter of a Cisco router that is running Cisco IOS Release 12.2(12a).

  Workaround: There is no workaround.

- CSCdz36099

  Symptoms: Web sites that require authentication become unreachable.

  Conditions: This symptom is observed on a router on which Web Cache Communication Protocol (WCCP) is enabled and Cisco Express Forwarding (CEF) switching is disabled. If the caches are Cisco caches, they will be running software prior to ACNS 4.2.5.

  Workaround: Ensure that CEF switching is enabled on the router. If this is not possible, the impact of the problem on the cache will be minimized if the authentication bypass function is disabled.

- CSCdz37137

  Symptoms: While Label Controlled ATM (LCATM), Tag Forwarding Information Base (TFIB), and Cisco Express Forwarding (CEF) all have the correct Label Virtual Circuit (LVC) information, the Label Distribution Protocol (LDP) path is broken. The **show xtagatm cross-connect interface**

xtagatmN EXEC command indicates that some cross-connects are in a "down" state. Errors in the controlled switch make the resynchronization of cross-connects fail.

Conditions: These symptoms are observed on a Cisco router that is used as a Label Switch Controller (LSC).

Workaround: There is no workaround. It is possible to recover from this condition by using the following commands:

- Use the **show xtagatm cross-connect interface xtagatmN** EXEC command to find all "down" cross-connects.
- Use the **show tag-switching atm-tdp binding** EXEC command to find the corresponding prefix/mask of the "down" cross-connects.
- Use the **clear ip route prefix** EXEC command for each prefix/mask.

- CSCdz37449

  Symptoms: A Route Switch Processor (RSP) may not forward Rendezvous Point (RP) announce packets to Protocol Independent Multicast (PIM) neighbors even though the egress interface is populated.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(10b).

  Workaround: Enter the **clear ip mroute *** EXEC command.

- CSCdz37574

  Symptoms: If a transient failure occurs in a Frame Relay network and causes three or more Voice over Frame Relay (VoFR) permanent virtual circuit (PVC) keepalive messages to be lost, the PVC will stop sending keepalive messages and will not start sending the keepalive messages again until the next outgoing call is placed. This behavior will occur if Frame Relay Local Management Interface (LMI) messages are not disturbed by the transient failure.

  Conditions: When the transient failure occurs, some PVC keepalives may be lost (but no LMI messages are lost) and PVC keepalives will be turned off. PVC keepalives should not be turned off when the transient failure occurs.

  The disabling of the PVC keepalives is not dependent on whether LMI messages are lost. If the transient failure persists for a sufficient period of time, LMI messages will be lost and Layer 2 will be marked down. When Layer 2 is marked down, PVC keepalives will also be turned off. The PVC keepalives will be restarted after Layer 2 recovery occurs.

  Workaround: There is no workaround.

- CSCdz37794

  Symptoms: After a Stateful Switchover (SSO) is performed on a Cisco 7500 series router whose incoming and outgoing interfaces are label-controlled ATM (LC-ATM) subinterfaces, it is possible for traffic to stop being passed through the router.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCdz38268

  Symptoms: A Cisco AS5350 that is running Cisco IOS Release 12.2(11)T may reload because of a bus error. This bus error is also seen on a Cisco AS5300 and Cisco AS5400 that is running Cisco IOS Release 12.2XB5.

Conditions: The bus error appears to be related to the Session Initiation Protocol (SIP) which is a text-based peer-to-peer protocol that allows user agents (UAs) to speak directly to other UAs or via the routing service of SIP servers called proxy and redirect servers.

The router configuration includes VoIP, FAX, and sip-ua.

Workaround: There is no workaround.

- CSCdz38742

  Symptoms: There may not be any label bindings on a Label Switch Router (LSR), but a Label Distribution Protocol (LDP) session may not be impaired.

  Conditions: This symptom is observed when an LDP session flaps quickly.

  Workaround: After the LDP session is brought down, remove all label bindings, and bring the session up again.

- CSCdz40015

  Symptoms: A Cisco AS5300 may reload because of a bus error, and the following error message may be generated:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x24, pc=0x60B2F64C,
  ra=0x60BA0798, sp=0x626EB378
  ```

  The output of the **show alignment** command does not display any information about the reload.

  Conditions: This symptom is observed on a Cisco AS5300 that is running the C5300-is-mz image of Cisco IOS Release 12.2(10a).

  Workaround: There is no workaround.

- CSCdz40331

  Symptoms: When an adjacent node connects to a Systems Network Architecture (SNA) switch, the following three errors may occur:

  - An incorrect mode name may be used in the incoming “Bind” message.
  - Control-point-to-control-point (CP-CP) sessions may no longer be supported.
  - Duplicate conversation group IDs may be used.

  When any of these errors occur, the SNA switch cannot recover from these errors and all subsequent CP-CP session activations from the adjacent node are rejected with sense code 08120010.

  Conditions: This symptom is observed on the SNA switch when the adjacent node generates one of the three above-mentioned errors.

  Workaround: Perform an Initial Program Load (IPL) of the SNA switch.

- CSCdz40483

  Symptoms: A Cisco router permanently pauses with a watchdog timer under normal operation.

  Conditions: This symptom is observed when the router is a voice endpoint with active calls.

  Workaround: There is no workaround.

- CSCdz42842

  Symptom: A Cisco 3640 may reload with a software-forced pause because of memory corruption.

  Conditions: This symptom is observed on a Cisco 3640 that is running Cisco IOS Release 12.2(8)T5 and that is configured with IPSec tunneling.

  Workaround: Do not configure the peer router to use IP subnet as an Internet Key Exchange (IKE) identity. Use the IP address or fully qualified domain name (FQDN) instead.

- CSCdz43056

  Symptoms: A high CPU utilization condition may be observed on a router.

  Conditions: This symptom is observed when the **debug atm oam** EXEC command is enabled and there is a large number of configured subinterfaces on a Cisco router.

  Workaround: Do not enable the **debug atm oam** EXEC command.

- CSCdz44138

  Symptoms: After a Session Initiation Protocol (SIP) message is received, a memory leak may occur in the CCSIP_SPI_CONTROL process on a Cisco MC3810 and the following errors are reported:

  - Method Not Allowed
  - Invalid CallId
  - Internal Server Error

  Conditions: This symptom is observed on a Cisco MC3810 that is running Cisco IOS Release 12.2(12).

  Workaround: There is no workaround.

- CSCdz45188

  Symptoms: When an incoming V.110 call fails on a Cisco 3600 series router, all subsequent incoming calls, including non-V.110 calls, may fail during the error correction (EC) negotiation.

  The output of the **show modem operational-status** *slot/port* EXEC command displays the following information:

```
Router# show modem operational-status 3/0
Modem (3/0) Operational Status:
Parameter #0 Disconnect Reason Info: (0x6210)
Type (=3 ): Condition occurred during call setup
Class (=2 ): EC condition - locally detected
Reason (=16): no EC fallback protocol available
```

  Conditions: This symptom is observed on a Cisco 3600 series router that is configured with a Terminal Adapter (TA) with a dialup setting of a third-party vendor.

  Workaround: Enter the **clear line** EXEC command.

  Alternate Workaround: Enter the **clear modem** EXEC command.

- CSCdz45785

  Symptoms: The **protocol ppp virtual-template** *number* interface configuration command may not function.

  Conditions: This symptom is platform independent and is observed in an environment that uses permanent virtual circuits (PVCs) or switched virtual circuits (SVCs).

  Workaround: There is no workaround.

- CSCdz48635

  Symptoms: A router that fulfills the very specific conditions listed below may reload unexpectedly with any of the following errors: a software-forced permanent pause, a watchdog timeout, or a bus error. These reloads may occur on all network access server (NAS) platforms for both voice and dial applications and all call types (CAS, analog, digital).

  Conditions: These symptoms are observed on routers that are running a Cisco IOS image that has the fix for CSCdt12536 but does not have the fix for CSCdz48635.

Workaround: There is no workaround.

- CSCdz49099

  Symptoms: After a few days, a Cisco 3660 router may stop routing calls properly from a PRI link. The calls will fail because the called number has been overwritten. The called number may be displayed correctly in the **debug voice ccapi inout** router output, but a different called number may be displayed in the **debug isdn q931** router output.

  Conditions: This symptom is observed on a Cisco 3660 router with a PRI link.

  Workaround: There is no workaround.

- CSCdz49276

  Symptoms: The gigabit interface of a Cisco Access Gateway Module (AGM) may reset and packets may be dropped. This behavior may cause poor voice quality and cause the AGM to be deregistered.

  Conditions: These symptoms are observed on a Cisco AGM that is using Cisco CallManager version 3.3.

  Workaround: Disable G.729 music on hold (MoH) on the Cisco CallManager.

- CSCdz50199

  Symptoms: A Versatile Interface Processor 2, Model 50 (VIP2-50) that is configured on a Cisco 7500 series router permanently pauses within a few minutes of loading. The following error message is shown:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0x60DC, ra=0x60DC, sp=0x6176C4B8
  ```

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(13.4)T. The symptom is not observed in Cisco IOS Release 12.2(12.14)T or prior releases.

  Workaround: There is no workaround.

- CSCdz51275

  Symptoms: A memory leak may occur in the process pool PC packet header and may cause a router to run out of memory.

  Conditions: This symptom is observed on a Cisco 2600 series. The more traffic the router passes, the quicker it runs out of memory.

  Workaround: There is no workaround.

- CSCdz51865

  Symptoms: A router may reload when more than two telnet sessions are established on a router and all sessions try to modify the same class map or policy map, or one session tries to modify the class map or policy map while another session is trying to access the data structures using the show command.

  Conditions: This symptom is observed on a router with more than two telnet sessions established.

  Workaround: While “showing” class map or policy map, do not modify or remove the data structure.

- CSCdz51932

  Symptoms: Deleting an access control list (ACL) that is used for IPSec may cause a router to reload.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 12.2(13.6).

  Workaround: Remove the crypto map from the interface before deleting the ACLs.

- CSCdz51987

  Symptoms: Concurrent mpls cos-map configurations may cause class commands entered by the first user to be applied to the incorrect class map.

  Conditions: This condition is observed on Cisco routers.

  Workaround: Restrict the **mpls cos-map** configuration to a single instance.

- CSCdz52774

  Symptoms: A router may reload because of illegal access to a low address. This symptom is observed if a particular race condition occurs when a delete context request is received by the Gateway General Packet Radio Service (GPRS) Support Node (GGSN) before a create response is sent back by GGSN for a packet data protocol (PDP) context.

  Conditions: This symptom is observed on a Cisco 7200 series that is running a GGSN image of Cisco IOS Release 12.2(12). This symptom is observed under a rare condition after RADIUS authentication and authorization have successfully occurred. Before a create response is sent, the process is suspended and a PDP context is deleted in a different process flow.

  Workaround: There is no workaround.

- CSCdz53326

  Symptoms: B channels may pause indefinitely in the “S_TSP_WAIT_RELEASE” state.

  Conditions: This symptom is observed on the B channels of a Cisco router that is running Cisco IOS Release 12.2(6c).

  Workaround: There is no workaround.

- CSCdz54206

  Symptoms: Packets are dropped when the **debug mpls packet** is enabled on a Route Switch Processor (RSP) on the outgoing interface while High-Level Data Link Control (HDLC) encapsulation is occurring.

  Conditions: This symptom is observed on Cisco routers that are running Cisco IOS Release 12.2, 12.2 T, and 12.2 S with the **debug mpls packet** command enabled.

  Workaround: Use the fast-switching path. Do not force the packets to take the Multiprotocol Label Switching (MPLS) process switch path (debug mpls packet.) Use the **ip cef distributed** global configuration command.

- CSCdz55608

  Symptoms: After a router is upgraded from Cisco IOS Release 12.2(10) to 12.2(12a), the router runs for about a day and then it pauses. The reason for this appears to be a memory leak in the crypto access control list (ACL). After a reboot, the router functions as expected, but after a number of hours the router get less and less responsive until it pauses.

  Conditions: This symptom is observed on routers that are running Cisco IOS Release 12.2. The routers may pause because of a memory leak on the “crypto ACL” process. This symptom is observed when the configuration has an ACL-less crypto map or a Tunnel End-Point Discovery (TED). This symptom is observed in Cisco IOS Release 12.2 images and not with flo_t images.

  Workaround: Use the (static) crypto map with ACL configured.

- CSCdz56072

  Symptoms: The dual-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX) used in a Versatile Interface Processor (VIP) on a Cisco 7500 series router will send 4 extra bytes at the end of the ethernet frames when configured with InterSwitch Link (ISL). This means that frames larger than 1496 bytes will be dropped as giants by the directly connected devices.

Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Releases 12.1(13.5)E or Release 12.1(13.5)1 with ISL configured. It is not observed in Cisco IOS Release 12.1(12.5)E1.

Workaround: Use dot1q encapsulation for trunking.

- CSCdz56722

  Symptoms: A Cisco 1700 series may reload because of a segmentation violation (SegV) exception.

  Conditions: This symptom is observed on a Cisco 1700 series that is running the c1700-k8o3sy7-mz image of Cisco IOS Release 12.2(13)T but may also occur in other releases such as Release 12.2 or Release 12.2 S.

  Workaround: Disable fast switching by configuring the **no ip route-cache** interface configuration command on the interfaces of the router.

- CSCdz57007

  Symptoms: A router may reload when a Multiprotocol Label Switching (MPLS) input feature (such as quality of service {QoS] classification, Qos marking, rate limiting, policing, or _expression bit accounting) or output features (such as QoS classification, QoS marking, rate limiting, policing, expression bit accounting, IP precedence accounting egress NetFlow, MPLS multi-virtual circuit [VC], Virtual Private Network [VPN] routing/forwarding Network Address Translation [VRF-NAT], or VRF-crypto) is configured on a router interface and when MPLS packets that are received by an MPLS router from the core are switched to the customer edge (CE) router through the VRF interface or to a local loopback under a deaggregation scenario.

  With certain Cisco IOS releases, the router reload may occur when certain types of Any Transport over Multiprotocol Label Switching (AtoM) disposition are performed. The reload can affect any platform that performs software MPLS switching.

  Conditions: This symptom is observed on a router that operates in an MPLS VPN environment.

  Workaround: There is no workaround. This symptom does not occur if input and output MPLS features such as the ones listed above are not configured on the PE router.

- CSCdz59578

  Symptoms: While switching from fax to voice, Cisco voice Gateways may experience DSP timeouts. This symptom occurs when the fax is over.

  Conditions: This symptom is observed when DSP is converting to voice mode from fax mode and the voice codec is G.728.

  Workaround: There is no workaround.

- CSCdz59591

  Symptoms: The append modifier does not append any data to named files on Advanced Technology Attachment (ATA) devices, and the original contents of the named file remain unchanged.

  Conditions: This symptom affects Cisco IOS releases that have the fix for CSCdz27200. This includes Cisco IOS Releases 12.2(13.7), 12.2(13.7)T, 12.2(13.7)S, 12.0(23.4)S, and 12.1(13.5)E1.

  Workaround: There is no workaround.

- CSCdz60229

  Symptoms: Cisco devices that run Cisco IOS software and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS software is disabled by default.

Conditions: This symptom is observed on all Cisco devices that run Cisco IOS software and contain support for the SSH server.

Workaround: Cisco will be making free software available to correct the problem as soon as possible.

The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml.

- CSCdz61466

  Symptoms: A Virtual Private Network (VPN) may stop working under rare traffic conditions.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13) and that is using one of the following VPN cards:

  - Basic performance VPN encryption asynchronous interface module (AIM-VPN/BP)
  - Enhance performance VPN encryption AIM (AIM-VPN/EP)
  - High performance VPN encryption AIM (AIM-VPN/HP)
  - Encryption NM (NM-VPn/MP)

  Workaround: Disable hardware encryption.

- CSCdz61744

  Symptoms: A router that is running many simultaneous PPP over ATM (PPPoA) sessions may observe the following error message and may occasionally reload.

  ```
  Vi1 PPP VA Err:pcr: Can't find phy iface.
  ```

  Conditions: This symptom is observed on routers that are running any Cisco IOS release; however, the symptom may not appear in older Cisco IOS releases or in situations with 2000 or fewer PPPoA sessions.

  Workaround: There is no workaround.

- CSCdz64355

  Symptoms: A router may reload.

  Conditions: This symptom is observed on a Cisco 7500 series router that has a Versatile Interface Processor (VIP) after the router is upgraded to Cisco IOS Release 12.2(12b). This symptom is observed if an ATM interface state changes while one or more permanent virtual circuits (PVCs) has the **random-detect** interface configuration command enabled.

  Workaround: Configure the **random-detect** interface configuration command under the modular quality of service (QoS) command-line interface (CLI).

- CSCdz65899

  Symptoms: The following CPU hog message may be displayed on a router after a multilink interface is shut down:

  ```
  %SYS-3-CPUHOG: Task ran for 2480 msec (3/2), process = Multilink
  ```

  Conditions: This symptom is observed when a state transition occurs on a multilink interface such as when the interface is coming up or going down.

  Workaround: There is no workaround for the CPU hog condition.

  If any application or routing protocol is affected by the CPU hog condition and is timing out because of the CPU hogging condition, increase the duration of the application or routing protocol timers.

- CSCdz68710

  Symptoms: When a policy that is attached to a large number of interfaces is removed, a watchdog timeout with some tracebacks occurs in the Route Processor (RP). It is also possible for the Versatile Interface Processor (VIP) or the router to permanently pause.

  Conditions: This symptom is observed when policies that are attached to a large number of interfaces are removed.

  Workaround: There is no workaround.

- CSCdz71171

  Symptoms: A router may report a loss of signal indication on all 28 T1 lines. When this symptom occurs, MIB updates that are being sent from a Route Switch Processor (RSP) to a Versatile Interface Processor (VIP) may stop.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(13)T and has channelized T3 (CT3) port adapters.

  Workaround: There is no workaround.

- CSCdz71295

  Symptoms: Poor voice quality occurs after several calls on a Cisco router.

  Conditions: This symptom is observed on a Cisco 7500 series router that is configured with Compressed Real-Time Protocol (CRTP) header compression.

  Workaround: Disable the CRTP.

- CSCdz71296

  Symptoms: A router may reload when a configuration command is being entered in the template submode.

  Conditions: If a user issues the **no template** configuration command to remove a template while another user is configuring the same template on the same router from another terminal, the router will reload.

  Workaround: Do not remove a template while other users are updating the configuration.

- CSCdz71663

  Symptoms: The output of the **test dsprm** hidden command and the output of the **show snmp** EXEC command display active digital signal processor (DSP) recovery alarms.

  Conditions: This symptom is observed on a Cisco AS5300 that is functioning as a voice gateway.

  Workaround: There is no workaround.

- CSCdz74211

  Symptoms: After starting Layer 2 (L2) and Layer 3 (L3) traffic, a Switch Processor (SP) or Route Processor (RP) may reload.

  Conditions: When L2 and L3 streams are started at the same time, the SP or RP may run out of interprocess communications (IPC) buffers and reload.

  Workaround: Manually increase the IPC cache size by using the **ipc cache 5000** global configuration command.

- CSCdz75118

  Symptoms: The interface input rate and output rate counters that are reported in the output of the **show interface** EXEC command do not decrease to zero after the interface is administratively shut down. The counters show the last input and output rates that were observed while the interface was up.

The following output may be observed when the **show interface serial 2/1/0** EXEC command is entered on the affected interface:

```
Router> show interface serial 2/1/0
Serial2/1/0 is administratively down, line protocol is dow
30 second input rate 466000 bits/sec, 560 packets/sec
30 second output rate 466000 bits/sec, 560 packets/sec
```

Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(13) and that has an Ethernet, Fast Ethernet, Gigabit Ethernet, ATM, Inverse Multiplexing over ATM (IMA), or serial interface. This symptom does not affect channelized serial interfaces.

Workaround: There is no workaround.

- CSCdz77618

  Symptoms: When a Gigabit Ethernet port adapter (PA-GE) card is removed from a Cisco 7200 series router that is configured with Gigabit Interface Converters (Gbics) to the PA-GE card with no cables attached, and then the PA-GE card is reinserted, the interface goes to an UP/UP state.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.1(11b)E3 or Release 12.1(13)E1.

  Workaround: There is no workaround.

- CSCdz78239

  Symptoms: A Cisco 7100 series router with the Integrated Service Module (ISM) card and Integrated Service Adapter (ISA) adapter intermittently resets.

  Conditions: This symptom is observed on a Cisco 7100 series router that is configured with an ISA adapter and ISM card and that is running Cisco IOS Release 12.1(14)E.

  After the ISA card reset message is displayed, the following occurs:

  – Some of the IPsec tunnels pause intermittently.
  – The **show crypto ipsec sa** EXEC command shows that the IPSec security associations (SAs) are running, but no encryption or decryption occurs.
  – Sometimes the router pauses immediately after the ISA card reset.

  Workaround: There is no workaround.

- CSCdz79023

  Symptoms: An ATM subinterface that is configured with switched virtual circuits (SVCs) pauses after the last SVC is cleared. The cleared interface remains in a paused state.

  Conditions: This symptom is observed on the interface when the last dynamic virtual circuit (VC) is deleted, and the interface is put in the paused state and does not recover.

  Workaround: Enter the **shut** interface configuration command followed by the **no shutdown** interface configuration command on the interface. SVC creation is then possible.

- CSCdz81035

  Symptoms: When a crashinfo file writes to an Advanced Technology Attachment (ATA) Flash disk, the file on the ATA Flash disk may be corrupt and unusable.

  Conditions: This symptom is observed on any Cisco device that enables the crashinfo file to be written to an ATA Flash disk.

  Workaround: There is no workaround.

- CSCdz84025

  Symptoms: A router will permanently pause as soon as the Cisco IOS software that has a code fix for the caveat CSCdz77618 is loaded. The following error message will occur as soon as the software image is loaded:

  ```
  *CWTLC PXF crash:Internal Error (0x00210001): Col0 CRASH_CODE_CMD_ID
  ```

  Conditions: This symptom is observed on all ethernet cards for the Cisco 7500 series routers.

  Workaround: There is no workaround.

- CSCdz85565

  Symptoms: A Cisco 7200 series router will cause IP Header Compression (IPHC) regression test failures.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.02(14.01). Because fast-switched packets are counted as process-switched packets, the symptom is observed only on M4T interfaces.

  Workaround: There is no workaround.

- CSCdz89370

  Symptoms: High-speed interfaces cannot be configured with the Quality of Service (QoS) feature for more than 14 percent of its link speed.

  Conditions: This symptom is observed only on a Cisco 7500series router that is running any Cisco IOS 7500 image, and when any QoS feature is configured with more than 428 Mbps.

  Workaround: There is no workaround.

- CSCea04706

  Symptoms: A Cisco AS5300 has calls failing with the following error message:

  ```
  'service/option not available' cause coe=0x3F
  ```

  Conditions: This symptom is observed on the digital signal processors (DSPs) on the voice feature card (VFC). The router is in the state "DSPRM-PLATFM: resource recovery" because of dangling DSPs.

  Workaround: Recover the DSPs to reduce the effect.

- CSCea06138

  Symptoms: After enabling CEF/tag switching, Route Switch Processor (RSP) routers will reload after applying the outgoing policy map.

  Conditions: This symptom is observed on Cisco RSP routers that are running Cisco IOS Release 12.2(15.1a).

  Workaround: There is no workaround.

- CSCea07020

  Symptoms: A Cisco router that is configured with Frame Relay (FR) subinterfaces may leak memory if the subinterfaces are configured with Random Early Detection (RED).

  Conditions: This symptom is observed when traffic shaping is configured with RED configured in the subclass in the service policy. If the subinterfaces are configured with RED, other changes to the configuration may cause the router to leak memory as well. For instance, adding an IP access list to a Frame Relay subinterface that is configured with RED will cause the router to leak memory.

  Workaround: There is no workaround.

- CSCea07570

  Symptoms: A Route Switch Processor (RSP) may permanently pause while sending Multiprotocol Label Processing (MPLS) packets over a Multilink PPP (MLP) interface.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(14.5)T.

  Workaround: There is no workaround.

- CSCea11008

  Symptoms: A Versatile Interface Processor (VIP) may permanently pause if the service policy that is attached to the virtual interface has a priority feature in it and the virtual interface is in the down state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: Remove the service policy from the interface before the interface goes down. Reattach the service policy after the interface is brought back up again.

- CSCea12346

  Symptoms: Applying a hierarchical service policy to a Frame Relay permanent virtual circuit (PVC) may cause incorrect bandwidth allocation among child classes. The **show policy interface** EXEC command may display incorrect bandwidth if the class is configured with "bandwidth percent" or "priority percent."

  Conditions: This symptom is observed if a hierarchical service policy is attached to a Frame Relay PVC in the following manner:

  ```
  policy-map child class voice priority percent 20
  policy-map parent class class-default shape average 1500000 service-policy child
  ```

  Workaround: There is no workaround.

- CSCin09506

  Symptoms: A Cisco 7200 series router may experience a permanent pause with the following error message:

  ```
  %ERR-1-SERR: PCI bus system/parity error
  %ERR-1-FATAL: Fatal error interrupt, reloading err_stat=0x88, err_enable=0xFF,
  mgmt_event=0x40
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.0 S, that has a PA-MC-8TE1+ port adapter configured in E1 mode with full channelization (248 interfaces), and that has framing as no-crc4 and line coding as AMI.

  Workaround: Do not allow full channelization (248 interfaces.) The T1 mode of operation is not affected.

- CSCin11687

  Symptoms: When primary and backup Non-Facility Associated Signaling (NFAS) controllers are configured on a PA-MCX port adapter, on shutting down the primary controller, Layer 1 of both the backup and primary controllers becomes deactivated. The backup D channel does not take over.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(10.5)T.

  Workaround: Enter the **no shutdown** interface configuration command, followed by the **shutdown** interface configuration command, followed again by the **no shutdown** interface configuration command on the serial interface of the primary controller.

Alternate Workaround: Configure primary and backup NFAS members on a PA-VXC port adapter and do not configure NFAS members on the PA-MCX port adapter.

- CSCin12517

  Symptoms: Some multilink interfaces may stop passing traffic.

  Conditions: This symptom may be observed when a router boots up or when the flexible WAN module (FlexWAN) is reloaded.

  Workaround: Manually reconfigure the multilink interface.

- CSCin15976

  Symptoms: A line card permanently pauses when a member link of a multilink bundle interface is removed and then put back.

  Conditions: This symptom may be observed only when “distributed crtp” is configured on the multilink interface and traffic is flowing through the multilink interface.

  Workaround: Shut down the multilink interface and then remove or add the member link.

- CSCin18275

  Symptoms: For nondistributed Cisco Express Forwarding (non-dCEF) 12x data forwarding on a Route Switch Processor (RSP), fast switching is used because l2x CEF switching is not supported by the platform. Because fast switching depends solely on the IP cache, any events that trigger IP cache flushing or a failure to update the IP cache lead to fast switching punting packets to the Route Processor (RP). With continuous traffic under this scenario, fast switching will allocate buffers for packet coalescing and queue them up for the RP to process. If the RP does not have a chance to process the packets fast enough, buffers will stay queued up while fast switching continues to allocate new buffers until the memory is exhausted.

  Conditions: This symptom is observed on an RSP after a minute of bidirectional traffic greater than 7 Mbps in each direction.

  Workaround: There is no workaround that completely eliminates this symptom. To decrease occurrences of the symptoms, avoid flapping interfaces and keep CPU utilization at a reasonable level (less than 80 percent). Use the **scheduler allocate** global configuration command to reserve some CPU cycles for RP processing.

- CSCin19132

  Symptoms: The **clear bridge** EXEC command can cause the cable modem to stop forwarding the traffic from the customer premise equipment (CPE) toward the cable interface.

  Conditions: This symptom is observed when the **clear bridge** command is executed more times than the number configured as max-cpe.

  Workaround: Shut down and bring up the cable interface with either the **shutdown** and **no shutdown** interface configuration commands or the **clear interface cable 0** interface configuration command.

- CSCin20858

  Symptoms: It is not possible to configure the following line cards:

  - OC-12 Packet-over-SONET (POS) line card
  - OC-3 POS line card
  - Gigabit Ethernet WAN (PWAN) line card

  Conditions: This symptom is observed when Cisco IOS image c6k222-jsv-mz.122-12.11.S is running and the router reloads without the startup configuration.

Workaround: Configure the G1/1 or G1/2 port. Save the configuration. Reload the system with the saved startup configuration. Once the system reloads, it is possible to configure the POS and PWAN interfaces.

- CSCin21005

  Symptoms: A mix of hairpin and Voice over IP (VoIP) calls fails with the following messages in the console:

  ```
  01:59:11: %VPA-3-TSBUSY: VPA (bay 4), TDM timeslot is busy: ST=13/TS=6 -Traceback=
  61164EEC 611655C4 6115D048 61157D50 61157EE0 61130F08 611315DC 61132DF4 61133618
  01:59:11: voice tdm connect failed(4/0/24/4/27/0)
  ```

  ```
  01:59:16: %VPA-3-TSBUSY: VPA (bay 4), TDM timeslot is busy: ST=13/TS=6 -Traceback=
  61164EEC 611655C4 6115D048 61157D50 61157FC4 611287A4 61141418 61141C48 6113323C
  61133618 01:59:16: voice tdm connect failed(4/1/5/4/27/0)
  ```

  ```
  01:59:17: %VPA-3-TSBUSY: VPA (bay 4), TDM timeslot is busy: ST=13/TS=6 -Traceback=
  61164EEC 611655C4 6115D048 61157D50 61157FC4 611287A4 61141418 61141C48 6113323C
  61133618 01:59:17: voice tdm connect failed(4/1/9/4/27/0)
  ```

  ```
  01:59:18: %VTSP-3-DSP_TIMEOUT: DSP timeout on channel 4/0:15:44083, event 6: DSP
  ID=0x1: DSP error stats, chnl info(4, 27, 0)
  ```

  Conditions: This symptom is observed on a Cisco 7200 series with voice port adaptors and occurs only when digital signal processors (DSPs) used for hairpin call setups are allocated for a new call before the hairpin call is completed.

  Workaround: There is no workaround.

- CSCin21199

  Symptoms: Spurious memory accesses may occur during the bootup process of a Cisco 7200 series router, or the router may reload during the bootup process.

  Conditions: This symptom is observed on a Cisco 7200 series router that is configured with an enhanced 8-port multichannel T1/E1 PRI port adapter (PA-MC- 8TE1+) configured in T1 mode and that is configured with a 2-port multichannel T1 port adapter (PA-MC-2T1), a 4-port multichannel T1 port adapter (PA-MC- 4T1), or an 8-port multichannel T1 port adapter (PA-MC-8T1).

  Workaround: There is no workaround.

- CSCin23256

  Symptoms: A router may reload when a microcode reload is performed.

  Conditions: This symptom is observed when the enhanced 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) of a Cisco 7500 series that is configured as either a T1 or an E1 port adapter is replaced by another port adapter.

  Workaround: There is no workaround.

- CSCin23875

  Symptoms: An outgoing gateway (OGW) sends the INVITE message with briefTags and the terminating gateway (TGW) is expected to respond with 100 “trying” and 180 “ringing” responses. However, the TGW ignores the INVITE message and treats it as a bad request.

  Conditions: These symptoms are observed on a Cisco AS5400.

  Workaround: There is no workaround.

- CSCin24544

  Symptoms: A permanent virtual connection (PVC) configuration is removed if a PVC fails when it is recreated.

Conditions: This symptom is observed on a Cisco 7500 series that has a Versatile Interface Processor (VIP). The PVC configuration may be removed if the VIP is carrying data traffic and the parameters of the virtual circuit (VC) class that is attached to the configured PVCs on the associated interface are modified.

Workaround: There is no workaround.

- CSCin24749

  Symptoms: A Versatile Interface Processor (VIP) on a Cisco 7500 series router may produce the following message upon insertion and removal of other VIPs:

  ```
  %VPA-3-CMDFAIL: DSPfarm4/1/2 Command Failed at ../src-rsp/rsp_vip_vpa.c - line 169,
  arg 2 -Process= "VTSP", ipl= 0, pid= 92
  -Traceback= 605021C8 605025D4 605030DC 60F4754C 60F423B0 60F42540 60F1C38C 60F1D460
  60F1DC64 voice tdm connect failed(9/0/26/9/24/0)
  ```

  Conditions: This symptom is observed on a Cisco 7500 series router with a PA-VXC-2TE1+ port adaptor.

  Workaround: Use online insertion and removal (OIR) of the VIP carrying PA-VXC-2TE1+.

- CSCin25008

  Symptoms: A Cisco 7500 series may reload.

  Conditions: This symptom is observed after an online insertion and removal (OIR) is performed on the Versatile Interface Processor (VIP) of a Cisco 7500 series. This symptom is observed if the 8-port T1 inverse multiplexing over ATM (IMA) port adapter (PA-A3-8T1) or the 8-port E1 IMA port adapter (PA-A3-8E1) is installed on the VIP.

  Workaround: There is no workaround.

- CSCin26592

  Symptoms: When multiple users configure a router, the router may reload.

  Conditions: This symptom is observed when configuring a Cisco router.

  Workaround: Do not attempt multiple user configuration on the same router.

- CSCuk39189

  Symptoms: Leaks may be observed for some Virtual Private Network (VPN) routing and forwarding (VRF) routes in the global Forwarding Information Base (FIB) table when a VRF is deleted and recreated.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0 S or 12.2 T.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCdy57048

  Symptoms: A Telnet session from a terminal over a vty connection to a Cisco 7206VXR router may pause indefinitely.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.2(4)XZ5, that is configured with a Network Processing Engine 300 (NPE-300), and that is functioning as a Multiprotocol Label Switching Virtual Private Network (MPLS VPN) provider edge (PE) router when large text displays are dumped on the screen of the terminal.

  The symptom is caused by a corrupt TCP Telnet packet that is generated by the router.

Workaround: There is no workaround.

- CSCdz20286

  Symptoms: A router that is running Cisco IOS software may reload.

  Conditions: This symptom may be observed when the following sequence of events occurs on the router:

  1. TCP intercept is enabled on the router via the **ip tcp intercept list** [*acl-number*] configuration command.

  2. TCP intercept is disabled on the router via the **no ip tcp intercept list** [*acl-number*] configuration command.

  3. TCP intercept is reenabled on the router via the **ip tcp intercept list** [*acl-number*] configuration command, and traffic matching the above access control list (ACL) is flowing through the router when this command is executed.

  Workaround: Make sure that no traffic matching the ACL is flowing through the router when TCP intercept is reenabled.

Wide-Area Networking

- CSCdu78087

  Symptoms: A "full" state may be displayed by the **show x25 hunt-group name** EXEC command for an interface participating in an X.25 hunt group when additional Virtual Circuits (VCs) are available. This symptom may cause all subsequent X.25 calls to use other interfaces that are participating in the hunt group.

  Conditions: This symptom may be observed when a Cisco router is configured for X.25 load balancing with hunt groups.

  Workaround: There is no workaround.

- CSCdx55019

  Symptoms: A router sends an exclusive "channel 0" SETUP message toward a PBX. The PBX responds with an "identified channel does not exist" message. This causes the PBX to drop the call.

  Conditions: This symptom is observed on a router that is configured with a BRI interface. The router sends a SETUP with exclusive "channel 0" in the SETUP for the BRI interface. A BRI interface should have only channel 1 or channel 2.

  Workaround: There is no workaround.

- CSCdy59613

  Symptoms: A software-forced reload error may occur on a router.

  Conditions: This symptom is observed when a dialer trigger call is made on platforms that support ISDN and dialer.

  Workaround: There is no workaround.

- CSCdy63773

  Symptoms: Call setup may not work as expected.

  Conditions: This symptom is observed on a vendor-specific private automatic branch exchange (PABX) after a connected Cisco router is upgraded to Cisco IOS Release 12.2(12).

  Workaround: There is no workaround.

- CSCdy70424

  Symptoms: A Cisco 7200 series router that is used in a Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) multihop setup as the PPTP Network Server (PNS) and L2TP Access Concentrator (LAC) node, and exhibits a combination of spurious memory accesses, packet misalignment warnings, and invalid TCP encapsulation errors and may permanently pause with a Translational Bridging (TLB) exception.

  Conditions: These symptoms are observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(10b). The spurious accesses and packet misalignments occur when the PPTP plus L2TP multihop setup is used. The invalid TCP encapsulations and the permanent pause occur when the number of sessions is high and some of the LNS routers are not reachable.

  Workaround: Do not use a combination of PPTP and L2TP protocols.

- CSCdy80595

  Symptoms: The Versatile Interface Processor (VIP) disabling feature is not working as expected. After the VIP reloads, it remains disabled even after an online insertion and removal (OIR) is performed on the VIP.

  Conditions: This symptom is observed when the OIR Remove Failing Slot (ORFS) feature is configured. The VIP is disabled after it reloads a certain number of times.

  Work around: Enter the **show rsp orfs-info** EXEC command to display the configured parameters for the service ORFS. After learning about the configured parameters for the service ORFS, the user may enter the **no service oir-remove-failing-slot** *slot number* **reload-limit** *reload-limit* global configuration command to enable a particular line card or enter the **no service oir-remove-failing-slot** global configuration command to enable all disabled cards.

- CSCdz03805

  Symptoms: A voice call that is placed over a Frame Relay link with Low Latency Queueing (LLQ) and Frame relay end-to-end fragmentation (FRF.12) enabled may permanently pause the router.

  Conditions: This symptom is observed on a router when the voice path is established with LLQ and fragmented data traffic active.

  Workaround: There is no workaround.

- CSCdz09265

  Symptoms: A Cisco Versatile Interface Processor 2 Model 40 (VIP2-40) may reload when a fragmentation configuration is removed.

  Conditions: This symptom is observed on a Cisco 7500 series that has a VIP2-40 interface that is running Cisco IOS Release 12.2(10b) and that is running Frame Relay and fragmentation.

  Workaround: Shut down the VIP2-40 interface before removing the fragmentation configuration.

- CSCdz12486

  Symptoms: X.25 does not permit a call confirmation to signal a source address other than the one that is specified in the original call (or the null address). The Cisco X.25 hunt group implementation will signal the modified source address back in the call confirmation when the source address of the call is modified by the route table. This behavior may cause the call to be cleared on a local procedure error.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13)T.

  Workaround: There is no workaround.

- CSCdz21325

  Symptoms: Incoming packets on a Cisco 3640 router are destined for a Cisco 2651 Modular Access Router via a Dial-on-Demand Routing (DDR) and BRI circuit. During failed BRI connection attempts (destination interface is shut), the memory in use increases steadily, incrementing with roughly every 3 to 6 packets sent.

  Conditions: This symptom is observed on a Cisco router and the memory leak is seen only when **isdn fast-rollover delay xy** is configured at the interface and the call fails at the first dial attempt.

  Workaround: Remove the **isdn fast-rollover delay xy** configuration.

- CSCdz25847

  Symptoms: The optional **priority** keyword of the **dialer pool-member** interface configuration command may not function properly, causing the command to select an incorrect interface.

  Conditions: This symptom is observed when two or more interfaces are configured as members of a dialing pool on a BRI interface.

  Workaround: There is no workaround.

- CSCdz44787

  Symptoms: After a router is reloaded, some multilink interfaces may be left in a state in which the line protocol stays down, even though the bundle interface is up.

  Conditions: This symptom is observed on high-end systems with many multilink groups of high-speed (T1 and above) interfaces.

  Workaround: Reset the bundle by issuing the **clear interface** interface configuration command on the multilink interface.

  Alternate workaround: Use the **shutdown** and **no shutdown** interface configuration commands to reload the router.

- CSCdz49773

  Symptoms: The **isdn map address** *address* **plan** *plan* **type** *type* interface configuration command may not be accepted when you enter **reserved** for the *type* argument.

  Conditions: This symptom is observed in an ISDN environment when ambiguity occurs with the value of the *type* argument (that is, the **reserved value**).

  Workaround: There is no workaround.

- CSCdz51400

  Symptoms: A router that is configured as a Home Gateway (HGW) may not correctly remove the per-user route.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.2(7c) or an earlier release and that is configured with per-user routes.

  Workaround: Reload the HGW.

- CSCdz58282

  Symptoms: A Versatile Interface Processor (VIP) with a synchronous serial port adaptor (PA-8T-V35) may permanently pause if a serial interface is configured for Frame Relay Fragmentation (FRF.11 Annex C).

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13)T or Release 12.2(13.4)T1.

  Workaround: There is no workaround.

- CSCdz61369

  Symptoms: A Cisco AS5300 reports the incorrect ISDN service status after a reload. When all of the B channels are set to maintenance state, the **show isdn service** EXEC command shows the correct information and all of the B channels are in maintenance state. After the router reloads with the same configuration, all of the B channels still show maintenance state except for the 24th B channel in the Non-Facility Associated Signaling (NFAS) group.

  Conditions: This symptom is observed on a Cisco AS5300 router that is running Cisco IOS Release 12.2(11)T and that is configured with Signaling System 7 (SS7) and NFAS.

  The output below shows the 24th B channel still in the service state.

```
5300# show isdn service

PRI Channel Statistics: ISDN Se0:23 SC, Channel [1-24] Configured Isdn Interface (dsl)
0 Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart 5=Maint_Pend) Channel
: 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 State : 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 Service State (0=Inservice 1=Maint 2=Outofservice) Channel : 1
2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 State : 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 0 Channel blocked? (0=No 1=Yes) Channel : 1 2 3 4 5 6 7 8 9 0 1 2 3
4 5 6 7 8 9 0 1 2 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

  Workaround: Add a command under the serial interface to put the channel into the maintenance state and confirm the change with the **show isdn service** EXEC command.

- CSCdz65823

  Symptoms: On a Cisco 6400 series router, the interface between the Node Switch Processor (NSP) card and the Node Route Processor (NRP) card may not show a consistent User-Network Interface (UNI) version configuration.

  Conditions: This symptom is observed if the NSP card is configured by default as "atm auto-configuration" and the NRP card has "atm auto-configuration" removed.

  Workaround: Leave "atm auto-configuration" configured on both the NSP and the NRP cards.

  Alternate workaround: Force the UNI version to choose one interface, and leave "atm auto-configuration" on the other card's interface.

  Additional workaround: Force both interfaces to the UNI version configuration.

- CSCdz66576

  Symptoms: When large numbers of Layer 2 Tunneling Protocol (L2TP) sessions are dropped, "thrashing" occurs with the virtual private dialup network (VPDN) history manager.

  Conditions: This symptom is observed on L2TP access concentrators (LAC) when the tunnels are shut down.

  Workaround: There is no workaround.

- CSCdz67847

  Symptoms: A router that is being used as an L2TP network server (LNS) may permanently pause for one of the following reasons:

  - redzone I/O memory corruption
  - a 64-K block move to an incorrect location
  - a 16 byte offset to the free I/O memory poi145
  - nter

  Conditions: These symptoms are observed when the LNS receives invalid length PPP packets.

  Workaround: There is no workaround.