Resolved Caveats—Cisco IOS Release 12.4(12c)

Cisco IOS Release 12.4(12c) is a rebuild release for Cisco IOS Release 12.4(12). The caveats in this section are resolved in Cisco IOS Release 12.4(12c) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCek47667

  Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

  Workaround: There is no workaround.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  Workaround: Add area 0 in the OSPF VRF processes.

  Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

Miscellaneous

- CSCsg99814

  Symptoms: On a router that functions in a GRE over IPSec or Virtual Tunnel Interface (VTI) configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface.

  Conditions: This symptom is observed when the ACL on the tunnel interface is configured on the outbound physical interface on which the IPSec tunnel is terminated.

  Workaround: Apply the outbound ACL on the protected LAN interface instead of on the tunnel interface.

- CSCsi27540

  Symptoms: A VSI session may become stuck in the “RESYNC_UNDERWAY” state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

  Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

Workaround: There is no workaround.

- 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

- CSCsi85641

  Symptoms: When the Reverse Route Remote Peer option is enabled, packets may not be forwarded correctly.

  Conditions: This symptom is observed when both CEF and the **reverse-route remote-peer** command are enabled. When you enable the **debug ip cef drops** command, typically, the following is shown:

  ```
  CEF-Drop: Stalled adjacency for remote-physical-ip-addr on Ethernet1/0
  for destination remote-protected-ip-addr
  CEF-Drop: Packet for remote-protected-ip-addr -- encapsulation
  ```

  Workaround: Disable CEF.

  Alternate Workaround: Add a next hop to the reverse route, for example, by entering the **reverse-route remote-peer** *ip-address* command.

Wide-Area Networking

- CSCsj10593

  Symptoms: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(15.6) and that functions as a TGW with all PRI switch types from the user to the network side. The symptom occurs when the **isdn test call interf ace** *interface-number dialing-string* command is entered at the platform on which the call is initiated, when the originating gateway (OGW) is configured for the National ISDN (primary-ni) switch type, and when the TGW is configured for the NT DMS-100 (primary-dms100) switch type. The symptom may also affect Release 12.4T.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(12b)

Cisco IOS Release 12.4(12b) is a rebuild release for Cisco IOS Release 12.4(12). The caveats in this section are resolved in Cisco IOS Release 12.4(12b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeb20967

  Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S, 12.1(14)E4, or 12.2 S when the following sequence of events occurs:

  1. A packet is switched via Cisco Express Forwarding (CEF).
  2. The egress interface has queueing/shaping configured.
  3. The egress interface is congested, causing the packet to be placed into the hold queue.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh80678

  Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(22) or a later release when the **auto-summary** command is enabled for BGP.

  Workaround: Enter the **no auto-summary** command.

- CSCsh90153

  Symptoms: Connectivity is lost through a router when traffic is processed twice by NAT.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(8a), that is configured for NAT and PBR, and that has a firewall feature enabled. Under certain conditions, traffic is processed twice by NAT when it does not need to be.

  Workaround: Remove the firewall configuration from the router.

  Further Problem Description: Syslogs and the output of the **show ip nat translation** command show that traffic that is processed twice by NAT does not traverse the router.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 12.2(18) and later.

  Workaround: Use ACLs to block invalid IP Control packets from reaching the control plane.

Miscellaneous

- CSCek38201

  Symptoms: A router may reload or display an alignment traceback when you enter the **show crypto socket** command.

  Conditions: This symptom is observed on a Cisco router that has an OSPFv3 IPSecv6 configuration.

  Workaround: There is no workaround. To prevent the symptom from occurring, do not enter the **show crypto socket** command in an OSPFv3 IPSecv6 configuration.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

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

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- CSCsf08998

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

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

- CSCsf28509

  Symptoms: When you enter the **clear ip dhcp binding** command to clear DHCP bindings, the corresponding DHCP-initiated subscriber sessions are not cleared.

  Conditions: This symptoms is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Enter the **clear ip subscriber** command to clear the subscriber sessions.

- CSCsg21401

  Symptoms: Calls may fail on a gatekeeper. When this situation occurs, you may not be able to Telnet or ping to the gatekeeper, and the logs of the gatekeeper contain several error messages with tracebacks that indicate "bad id in id_get". In addition, gateways may also unregister from the gatekeeper.

  The following error message and traceback are generated when the symptom occurs:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x6445D720)
  -Traceback= 0x6114DA04 0x622C7944 0x610F767C 0x610F8228 0x610F8138 0x6110C854
  0x6110CBB8 0x60074F1C 0x60063D74 0x60040B94 0x60052A84 0x6002637C 0x60028AB0
  ```

  Symptoms: This symptom is observed on a Cisco platform that functions as a gatekeeper in an H.323 environment.

  Workaround: There is no workaround.

- 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.

- CSCsg59326

  Symptoms: When an ATM (that is, a cash machine, not a WAN platform) is connected to a switch service module, significant packet loss may occur.

  Conditions: This symptom is observed on a Cisco 2800 series router.

  Workaround: Change the Ethernet speed to 10 Mbps at both ends.

- 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

- CSCsg78414

  Symptoms: A sweep ping with a size of 4571 bytes may fail.

  Conditions: This symptom is observed on a Cisco 7500 series when an ATM-IMA interface is configured with an MTU size of 7000 bytes.

  Workaround: There is no workaround.

- CSCsg96319

  Symptoms: Anyone can have unprivileged Telnet access to a system without being authenticated, when a reverse SSH session is established with valid authentication credentials. This only affects reverse SSH sessions where a connection is made with the command **ssh -l** *userid***:***number ip-address* command.

  Conditions: This symptom has been seen only when Reverse SSH Enhancement is used. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhanmt_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  Workaround: Configure reverse SSH with the **ip ssh port** *portno* **rotary** *rotarygroup* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- CSCsh33430

  Symptoms: A traceback may occur in an HSRP function and the platform may reload unexpectedly.

Conditions: This symptom is observed on a Cisco platform that has the HSRP Support for ICMP Redirects feature enabled and occurs when a learned HSRP group is removed after a resign message has been received.

Workaround: Disable the Support for ICMP Redirects feature by entering the **no standby redirects** global configuration command.

- CSCsh75827

  Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the "J" Service-Info attribute), has logged out from the SESM, and then renews its IP address.

  Workaround: There is no workaround.

- CSCsh92914

  Symptoms: A router may unexpectedly reload when you attempt to open a reversed SSH connection by using the SSHv1 protocol.

  Conditions: This condition is observed on a Cisco router that runs Cisco IOS Release 12.4.

  Workaround: Force the SSH transport to be SSHv2 by entering the **ip ssh version 2** global configuration command.

- CSCsh94526

  Symptoms: When an acct-stop message is received for a non-RADIUS proxy user (that is, a normal IP user), a router that is configured for SSG crashes.

  Conditions: This symptom is observed when SSG is configured for RADIUS proxy mode and when the **ssg wlan reconnect** command is enabled.

  Workaround: There is no workaround.

- CSCsh97579

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi04707

  Symptoms: Configuring an AUX port for async interface through a non-slotted notation such as the **interface async 1** command or slotted notation such as the **interface async x/y/z** command may not be possible on a Cisco 2851.

Conditions: This symptom has been observed on a Cisco 2851 router with Cisco IOS Release 12.4(13). This symptom has not been seen on Cisco IOS Release 12.4 (10) and earlier.

Workaround: There is no workaround.

- CSCsi27767

  Symptoms: One-way audio may occur when a call is transferred or picked up after having been on hold.

  Conditions: This symptom is observed intermittently on a Cisco Communication Media Module (CMM) for calls that are transcoded because of a transfer or being placed on hold and for which the RTP stream terminates on the CMM.

  The symptom appears to occur because of a significant change in the sequence numbers and timestamp of the RTP packets while the same SSRC is kept. You can identify this situation with a packet capture of the RTP stream.

  Workaround: There is no workaround.

- CSCsi42086

  Symptoms: A memory leak may occur on a router that is configured for SSG when unsupported 3GPP attributes are received by SSG.

  Conditions: This symptom is observed when SSG is configured to function in RADIUS proxy mode.

  Workaround: Ensure that the unsupported 3GPP attributes are removed by filtering them before a RADIUS packet is received by SSG.

TCP/IP Host-Mode Services

- CSCsi40766

  Symptoms: H.323 calls on a Cisco IOS VoIP gateway may fail after the gateway has processed about 54,500 calls.

  Conditions: This symptom is observed when H.323 uses TCP to transport signaling messages. When the Cisco IOS gateway must generate a unique port for the local TCP session, this port is selected from a range of open ports. When the number of times that an unique TCP session is created for the same IP address on the gateway exceeds 54,500, further attempts to create a local TCP port fail and calls are not completed.

  The symptom occurs for H.323 calls only when a separate TCP session is established for the H.245 session. When H.245 tunneling is enabled or no H.245 session is established, the symptom does not occur for H.323 calls.

  When the **debug ip tcp transaction** command is enabled on the gateway, the "TCP: Ran out of ports for network 0" debug output is generated when the symptom occurs.

  Enabling debugs on a Cisco IOS gateway should always be done with caution to minimize impact to the performance of the router. As a minimum, ensure that logging to the console is changed from the default behavior of the debug level to, for example, an informational level.

  Workaround: After the symptom has occurred, reload the Cisco IOS VoIP gateway. To prevent the symptom from occurring, ensure that for H.323 call processing all H.323 devices have H.245 tunneling enabled. This may not always be possible: for example, H.245 tunneling on Cisco CallManager is not supported.

Wide-Area Networking

- CSCsh82513

  Symptoms: The output of the **show isdn active** command may show disconnected calls.

  Conditions: This symptom is observed on a Cisco router when analog modem calls are made after a normal ISDN digital call has been made.

  Workaround: There is no workaround.

- CSCsi21853

  Symptoms: When you attempt to change the ISDN T306 timers, the changes are not accepted.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4.

  Workaround: There is no workaround.

  Further Problem Description: The ISDN T306 configuration updates the values of the ISDN T307 timers.

Resolved Caveats—Cisco IOS Release 12.4(12a)

Cisco IOS Release 12.4(12a) is a rebuild release for Cisco IOS Release 12.4(12). The caveats in this section are resolved in Cisco IOS Release 12.4(12a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsg21398

  Symptoms: Cisco IOS may restart when receiving a crafted TACACS+ msg-auth-response-get-user packet after it sends out an initial TACACS+ recv-auth-start packet.

  Workaround: There is no workaround.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  – You reload the router.

  – A switchover of the active RP occurs.

  – You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. Is this not an option, there is no workaround.

- CSCsh44174

  Symptoms: After a router has crashed, another crash may occur while the crashinfo is being generated, and a traceback with memory addresses is displayed.

  Conditions: This symptom is observed on a Cisco router when, during the crash, the data in key memory locations is written to a crashinfo file on the bootflash device of the router.

  Workaround: Specify an alternate storage device to store the crashinfo in the startup configuration, for example, by adding the following line to the startup configuration:

  exception crashinfo disk0:

- CSCuk61422

  Symptoms: CEF-switching does not function, and the output of the **show adjacency** *interface interface-number* **detail** command does not show any packets.

  Conditions: This symptom is observed on a Cisco 7500 series that has an RSP when packets are switched to a multilink interface via CEF and when you enter the **show adjacency** *interface interface-number* **detail** for a multilink interface.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCse97264

  Symptoms: Two or more UDP NAT translations that relate to different requests may be assigned port numbers with the same inside global IP address.

  Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.3(11)T9 when more than one IP phone attempts to register through a router that is configured for NAT Overload.

  Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsg48509

  Symptoms: The **match-in-vrf** keyword is missing from the **ip nat inside source** command, and the **ip nat inside source** command is not accepted at all in interface-configuration mode.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(11.6a) or interim Release 12.4(12.03)T but may also affect other routers.

  Workaround: There is no workaround.

- CSCsg50321

  Symptoms: A router may hang when you enter the **clear ip nat translation *** command.

  Conditions: This symptom is observed on a Cisco 7500 series that has an RSP when you configure static NAT for an inside source address.

Workaround: There is no workaround.

- CSCsg84883

  Symptoms: NAT configurations are not removed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

ISO CLNS

- CSCsg28497

  Symptoms: An IS-IS adjacency may flap when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco router that is configured for IS-IS Multi-Topology, IS-IS NSF Awareness, and IPv4 and IPv6 unicast.

  Workaround: There is no workaround.

Miscellaneous

- CSCds25257

  Symptoms: Gatekeeper Rejects new registration requests from CUCM or other H.323 endpoints with RRJ reason of duplicateAlias. Attempting to clear this stale registration fails with “No such local endpoint is registered, clear failed.” message.

  Conditions: CUCM H.225 trunks register to a gatekeeper (GK) cluster. GK1 and GK2 are members of the GK cluster. CUCM registers first to GK1 then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

  Once the H.225 trunk attempts to register with GK1, it gets rejected because the alternate registration is still present, and there is no way to clear it out.

```
10.9.20.3       34273 10.9.20.3       32853 SJC-LMPVA-GK-1    H323-GW A
    ENDPOINT-ID: 450FC24400000000  VERSION: 5  AGE: 1618993 secs
SupportsAnnexE: FALSE
    g_supp_prots: 0x00000050
    H323-ID: SJC-LMPVA-Trunk_4
```

  Workaround: Reset the gatekeeper with the **shutdown** command followed by the **no shutdown** command, or reboot the Cisco IOS GK.

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- CSCed57504

  Symptoms: A router that is configured with a virtual template may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router on which a session that uses a virtual-template is terminated and occurs when the session is cleared from a DSL CPE router that is the peer router for the connection.

  Workaround: There is no workaround.

- CSCek48251

  Symptoms: When you enter the **redundancy switch-activity force** command on the active eRSC of a Cisco AS5850 while incoming VoIP H.323 calls and outgoing CAS calls are being processed, the standby eRSC does become the active eRSC and processes the calls but soon afterwards may crash at "csm_enter_idle_state."

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(9)T and that functions in RPR+ mode. The symptom may also affect Release 12.4.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRI calls are being processed.

- CSCek55511

  Symptoms: A Cisco AS5400HPX that is running Cisco IOS Release 12.3(11)T7 may crash with IO Memory corruption.

  Conditions: The crash may occur when polling for ccrpCPVGEntry, and resource pooling is enabled on the Gateway.

  Workaround: Disable SNMP polling for ccrpCPVGEntry.

- CSCsg05350

  Symptoms: A Cisco platform crashes due to a chunk memory leak and generates the following error messages and tracebacks:

  ```
  %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a reload due to
  Fragmented processor_memory, Free processor_memory = 10402472
  bytes, Largest processor_memory block = 522632 bytes
  ```

  Conditions: This symptom is observed on a Cisco AS5850 when there is a chunk memory leak. However, the symptom is platform-independent and relates to the Distributed Stream Media Processor (DSMP).

  Workaround: There is no workaround.

- CSCsg08395

  Symptoms: When one of the controllers of a VWIC-2MFT-E1 Voice/WAN interface card that is connected back-to-back to another router is shut down, ISDN L2 may go down on the second E1 controller of the VWIC-2MFT-E1.

  Conditions: This symptom is observed on a Cisco 3725 that runs Cisco IOS interim Release 12.4(11.1).

  Workaround: There is no workaround.

- CSCsg28628

  Symptoms: NAS pkg asynchronous calls fail after a redundancy switchover has occurred, and the following error message is generated:

  Modems unavailable

  Conditions: This symptom is observed on a Cisco AS5850 that functions in RPR+ mode. This situation may impact service.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **redundancy switchover** command a couple of times to restore the Cisco AS5850 to normal operation.

- CSCsg37423

  Symptoms: The output of the **show l2tun session l2tp** command does not include interface information.

  Conditions: This symptom is observed on a Cisco router that is configured for Xconnect.

  Workaround: There is no workaround.

- CSCsg39287

  Symptoms: A memory leak and fragmentation may occur on a terminating H.323 gateway upon receipt of an H.225 Notify message, and the gateway may crash.

  Conditions: This symptom is observed on a Cisco AS5400 that has been processing calls for a couple of days.

  Workaround: There is no workaround. There would be a workaround if you could prevent the originating device from sending Notify messages. However, this is not an option in a typical Cisco CallManager IP Telephony (IPT) deployment.

- CSCsg50187

  Symptoms: CEF-switching does not function, and the output of the **show adjacency** *interface interface-number* **detail** command does not show any packets.

  Conditions: This symptom is observed on a Cisco router when packets are switched to a multilink interface via CEF and when you enter the **show adjacency** *interface interface-number* **detail** for a multilink interface.

  Workaround: There is no workaround.

- CSCsg58832

  Symptoms: Inconsistent lease times may occur on a router that functions as a DHCP relay agent. The lease expiration times may be reduced from the value that is specified by the server to as little as five minutes. After the new lease time has expired, the binding is then deleted.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T, that is configured as a DHCP relay agent, and that has the **ip dhcp smart-relay** command enabled.

Workaround: Remove the **ip dhcp smart-relay** command from the configuration.

Alternate Workaround: Renew the IP address on the DHCP client.

- CSCsg69124

  Symptoms: A router crashes when the **write memory** and **secure boot-image** commands are executed simultaneously.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

  Further Problem Description: Note that the commands must be entered simultaneously for the symptom to occur. When the commands are entered one after the other (in any order), the symptom does not occur.

- CSCsg69205

  Symptoms: On a Cisco PE router that has the **ip flow egress** command enabled on an interface that connects to a CE router, the traffic streams that are destined for the CE router may not be captured.

  Conditions: This symptom is observed when the MPLS interface is a multilink interface.

  Workaround: Enter the **mpls netflow egress** command on the interface that connects the PE router to the CE router to enable the traffic streams to be captured by NetFlow. Once the traffic streams are being captured you can remove this command.

- CSCsg76715

  Symptoms: A device crashes when you delete an ACE that was inserted in the middle of the ACL rather than added at the end of the list.

  Conditions: This symptom is observed when all of the following conditions are present:

  – The inserted ACE has a destination prefix length of 0, that is, is has an “any” statement instead of a destination address.

  – The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an “any” statement), and the inserted ACE has a lower sequence number than this other ACE.

  – The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

  Workaround: First, delete the inserted ACE. Then, delete the other ACE with the same SRC prefix length and an destination prefix length that is greater than 0.

  Alternate Workaround: Delete the complete ACL.

- CSCsg81585

  Symptoms: After you stop sending stress traffic, an egress interface of an NM-4A/S stops sending all packets, that is, the output becomes stuck.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  – MLP is configured.

  – There is an asynchronous physical layer on the serial interfaces.

  – A dialer session is established by the stress traffic.

  Workaround: Enter the **no ip route-cache** command on the egress interface of the NM-4A/S. Note that doing so may increase the CPU usage.

- CSCsg96462

  Symptoms: A memory leak may occur in the SNASwitch process.

  Conditions: This symptom is observed when the SNASwitch fails to free memory that is associated with maintaining the RTP history information when RTP pipes terminate under some conditions.

  Workaround: There is no workaround.

  Further Problem Description: The following messages may be generated when the processor memory has been exhausted:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x6016CEA0,
  alignment 0
   Pool: Processor  Free: 1628716  Cause: Memory fragmentation
   Alternate Pool: None  Free: 0  Cause: No Alternate pool
   -Process= "SNA Switch", ipl= 0, pid= 64
  ```

  To check if memory is leaking, enter the following commands (note the exact upper/lower cases that are used):

  ```
  show snasw rtp
  show memory summary | i GraphIt | Bytes
  ```

  The first command displays all the RTP pipes. The second command displays a summary of all the memory with a “GraphIt” identifier. There should be approximately two blocks with the “GraphIt Client” identifier for each non-RSETUP RTP pipe.

  If there are significantly more than two “GraphIt Client” blocks per RTP pipe, the SNASwitch is leaking memory.

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

  ```
  %MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of
  [dec] - VRF [chars]
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

  Workaround: There is no workaround.

- CSCsh58082

  Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

  There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

  Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

Wide-Area Networking

- CSCek59078

  Symptoms: An L2TPv3 session is established when voluntary tunneling is configured and both peers have corresponding configurations. However, after you configure a pseudowire on a virtual PPP interface on one of the peers, the session on this peer is up but the line protocol is down, an a "virtual-PPP1 is up, line protocol is down" error message is generated.

  Conditions: This symptom is observed when the virtual PPP interface is first deleted via the **no interface virtual-ppp** *number* command and then reconfigured via the **interface virtual-ppp** *number* command before you configure a pseudowire on the virtual PPP interface.

  Workaround: Before you configure a pseudowire on the virtual PPP interface, ensure that the virtual PPP interface has never been unconfigured via the **no interface virtual-ppp** *number* configuration command.

- CSCek60025

  Symptoms: A ping may be dropped in a PPP callback scenario.

  Conditions: This symptom is observed on a Cisco router when Multilink PPP (MLP) and the **dialer load-threshold** command are enabled.

  Workaround: There is no workaround.

- CSCek60772

  Symptoms: A crash occurs when commands are executed in a particular order.

  Conditions: The crash occurs when the following commands are executed:

```
interface Dialer0
no dialer pool 1
shut
no interface Dialer0

interface Serial2/0
no dialer in-band

interface Dialer0
dialer remote-name dt3b7-4
no cdp enable
```

  This happens because a freed value was not being set to NULL.

  Workaround: There is no workaround

- CSCek62099

  Symptoms: When Multilink PPP (MLP) is enabled for a PPP over Ethernet (PPPoE) session, outbound packets are incorrectly sent without PPPoE headers. This situation causes packets to be dropped.

  Conditions: This symptom is observed in Cisco IOS Release 12.4 on all software-forwarding routers and affects only packets that are not multilink-encapsulated (when the bundle has only a single link).

  Workaround: Enter the **ppp multilink fragment delay** interface configuration command to force multilink headers to be applied to all outbound packets.

  Alternate Workaround: Disable MLP.

- CSCsb24255

  Symptoms: A router may generate the following error message and a MALLOC failure may occur:

  ```
  flex_dsprm_voice_connect: voice tdm connect failed
  ```

  Conditions: This symptom is observed on a Cisco router that processes a large number of calls with a short call duration via an E1 PRI.

  Workaround: There is no workaround.

- CSCsf30493

  Symptoms: When a T.37 onramp call is made, the following error message may be generated:

  ```
  %CSM-3-NO_VDEV: No modems associated
  ```

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS interim Release 12.4(10.7). The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg40885

  Symptoms: A router crashes during an online insertion and removal (OIR) of a multilink interface.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for MLP and PPP.

  Workaround: Shut down the multilink interface before you perform an OIR.

- CSCsg50202

  Symptoms: When a BRI interface flaps rapidly, ISDN Layer 1 detects a link down state, but Layer 2 and Layer 3 may remain in the active state during the transition. This situation may cause the BRI interface to become stuck, and subsequent incoming and outgoing calls to be rejected.

  Conditions: This symptom is observed when a cable is pulled out and put back rapidly.

  Workaround: Enter the **clear interface** command on the affected BRI interface.

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

- CSCsg56148

  Symptoms: Inbound GSM V.110 calls fail to train at a speed of 14400 bps.

  Conditions: This symptom is observed on a Cisco AS5400 when the Bearer Capability (BC) does not match the Lower Layer Compatibility (LLC) in the ISDN setup message. The BC should take precedence over the LLC.

  Workaround: If this an option, configure the ISDN switch to send the correct BC and LLC. If this is not an option, there is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(12)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(12). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(12). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCek40101

  Symptoms: If a Cisco 2800 series router is configured to do async tunneling using sync/async module with very slow speed like 2400bps or below, the sync/async line may get in stuck state. Entering the **show tcp** command on that stuck line shows CLOSED TCP connection with some unread input bytes, for example:

  ```
  Router#sh tcp
  tty0/2/0, connection 1 to host 172.16.242.129
  Connection state is CLOSED, I/O status: 7, unread input bytes: 97
  Connection is ECN Disabled
  Local host: 172.16.146.249, Local port: 20514
  Foreign host: 172.16.242.129, Foreign port: 23
  ....
  ....
  ```

  Conditions: This symptom occurs only when the Cisco 2800 series router is used for async data tunneling at line speed of 2400 bps or lower with wic-2a/s card

  Workarounds: See the following:

  1. Issue the **clear line** *x/y/z* command to make that line usable again
  2. Use Cisco IOS Release 12.3(14)T7, which does not show this issue as readily as Cisco IOS Release 12.4.
  3. Use line speed higher than 2400 bps.
  4. Use aux port of 2800 router.

- CSCir00074

  Symptoms: A router crashes when the casnDisconnect object is set to "true" for a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series when you attempt to terminate the PPPoE session through SNMP by using the casnDisconnect object of the CISCO-AAA-SESSION-MIB.

  Workaround: There is no workaround.

- CSCsd26248

  Symptoms: A memory leak may occur in the RADIUS process on a router that is configured for dot1x authentication but that does not have the **aaa authentication dot1x** command enabled. The memory leak may consume all free memory.

  Conditions: This symptom is observed when the router receives attribute 24 (state) or attribute 25 (class) from a RADIUS server.

  Workaround: There is no workaround.

- CSCsd90876

  Symptoms: Memory corruption occurs when a "| include" is used with a CLI command. An already in-use block gets freed and causes this corruption.

  Conditions: This symptom can happen with any usage when a "| include" is used with a CLI command. It was found using a script for IPSec that resulted in "Crash on OIR of IPSec SLC module."

  Workaround: There is no work around. It is a programming defect.

  Further Problem Description: It is a rare corner case memory corruption when a block gets freed even when it is in use. It is caught by a script under stress testing conditions which results in such a rare condition. While using CLI and "| include" it is rare to get such a corruption. If it happens, it will lead to box reload.

- 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.

- CSCse79528

  Symptoms: Serial and FDDI interfaces may not be detected.

  Conditions: This symptom is observed only on a Cisco 7500 series that has an RSP.

  Workaround: There is no workaround.

- CSCse85200

  Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour 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.

- CSCse90357

  Symptoms: Onramp and offramp fax calls fail to connect over E1 PRI and E1 R2 signaling.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

- CSCse90580

  Symptoms: A Cisco router may crash due to a bus error while removing the **ip flow egress** command from an interface.

  Conditions: The router must have the **ip flow egress** command previously configured on the interface.

  Workaround: There is no workaround.

- CSCsf19139

  Symptoms: %RADIUS-3-NOSERVERS messages are logged after a reload in Cisco IOS Release 12.3(18). At this time, the RADIUS accounting tickets are not generated.

Conditions: This symptom has been observed on a Cisco AS5300 gateway.

Workaround: Enter into configuration mode and change the order of the servers under the server group.

- CSCsf32390

  Symptoms: When tuning particle clone, F/S, and header pools after these were made configurable via CSCuk47328, the commands may be lost on a reload.

  Conditions: If the device is reloaded the commands are not parsed on a reload and this results in the defaults being active. This may result in traffic loss if the increased buffers were needed to enable greater forwarding performance for the specific network design.

  Workaround: Configure an applet to enter the buffer values again after a reload. A sample applet would be:

```
event manager applet add-buffer
 event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "buffers particle-clone 16384"
 action 4.0 cli command "buffers header 4096"
 action 5.0 cli command "buffers fastswitching 8192"
 action 6.0 syslog msg "Reinstated buffers command"
```

EXEC and Configuration Parser

- CSCse77357

  Symptoms: A router may reject the creation of virtual Token Ring interface with any interface number from 0 to 9 and allow only the creation of virtual Token Ring interface with an interface number that is equal to or greater than 10.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.16) or a later release or Release 12.4(9.15)T or a later release.

  Workaround: Manually configure the virtual Token Ring interface with a an interface number that is equal to or greater than 10.

Interfaces and Bridging

- CSCsd74009

  Symptoms: In a Cisco 7500 router with PA-2FE, when entering the **shutdown** command and then the **no shutdown** command on the current exit interface (PA-2FE) of the Border Router (Cisco 7500 series), the Border Router may not come to ACTIVE state on the MC.

  Condition: This symptom has been seen in RSP routers with PA-2FE interface only.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCek14600

  Symptoms: A traceback has been seen on this release.

  Conditions: The symptom has been observed on Cisco IOS interim Release 12.4(04) T1fc2.

  Workaround: There is no workaround.

- CSCek27981

  Symptoms: The output of the ping is different than expected.

  Conditions: This symptom has been observed after configuring the security options when the output of the ping is different than expected.

  Workaround: There is no workaround.

- CSCek51676

  Symptom: Router crash on watchdog timeout.

  Condition: Delete lots of interfaces with interface range command.

  Workaround: There is no workaround.

- CSCse29428

  Symptoms: A crash is seen with %ALIGN-1-FATAL after showing %SYS-2-CHUNKEXPANDFAIL and %SYS-2-MALLOCFAIL repeatedly.

  Conditions: This symptom is observed on a Cisco 3725 router that is running Cisco IOS Release 12.4(5a) with the c3725-advipservicesk9-mz image that is running IPSec VPN.

  Workaround: There is no workaround.

- CSCse56552

  Symptoms: Connections fail through a router that uses CBAC. The pre-gen session is created, and the download or transfer begins. The pre-gen session times out and gets deleted from the router. Since the full session never gets established, the connection then times out on the host.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(8) and using CBAC outbound on the outside interface when policy based routing is applied.

  Workaround: There is no workaround.

  Further Problem Description: This bug was first seen in Cisco IOS Interim Release 12.4(7.24).

- CSCse58419

  Symptoms: The memory consumption by the Chunk Manager process increases over time.

  Conditions: This behavior is observed on certain occasions when NAT is configured. When NVI with VRF is set in the system, the memory leaks rapidly. When NAT with VRF is set in the system, plus there is embedded address translation needed or skinny protocol traffic, the memory leaks in a slow pace.

  Workaround: There is no workaround.

- CSCse78454

  Symptom: Two OSPFv3 interface commands:

  ```
  ipv6 ospf <PID> area <area ID>
  ipv6 ospf neighboor <address>
  ```

  can disappear after ION process iprouting. iosproc crash or restarted.

Conditions: This symptom has been observed only with ION image.

Workaround: There is no workaround.

- CSCse94682

  Symptoms: A Cisco router with EIGRP configured might generate an error message like:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6097922C reading 0x70
  ```

  Conditions: The symptom only occurs if the **no ip next-hop-self eigrp** command is configured.

  Workaround: There is no workaround.

- CSCse98590

  Symptoms: The router will display SYS-2-MALLOCFAIL messages on the console, and various protocols will operate erratically as a result of a low memory condition.

  Conditions: When a router has to duplicate incoming IPv4 multicast packets for transmission on multiple interfaces, and one of those interfaces is a GRE tunnel operating in GRE IPv6 mode, then memory used to duplicate that packet stream will not be freed. As a result, the router will soon exhaust all available memory.

  Workaround: The router will not exhaust memory if packets do not need to be duplicated (for example, if they enter on one interface and only exit the box through another interface), or if they do not need to duplicate to a tunnel interface that is running GRE over IPv6 (for example, tunnel mode GRE IPv4 does not have this problem).

- CSCse98834

  Symptoms: When SNAT is configured and mapping-id is only added to static NAT statements, Dynamic NAT entries do not time out.

  Workaround: Add mapping-id to dynamic NAT config if possible.

- CSCsf02935

  Symptoms: A router that is configured for OSPF Sham-Link and BGP redistribution may crash.

  Conditions: This symptom is observed only in network topologies with OSPF routes that traverse two or more sham links. For example, the symptom may occur in a hub-and-spoke topology with sham links between the hub and two or more individual spokes. This symptom was observed on a Cisco 10000 series but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCsg00860

  Symptoms: Enabling NAT outside on the public interface terminates the VPN connection as GREoverIPSEC. Inbound ACL applied on the public interface starts to drop decrypted GRE traffic.

  Conditions: This symptom has been observed with the use of IP NAT outside on the public VPN interface.

  Workaround: There are 2 workarounds:

  1. Configure NAT translations for all traffic, to force NAT processing on the packet even if no address will actually be translated. Example:

     ```
     ip nat inside source static 171.16.68.5 171.16.68.5
     ```

     It is not a scalable workaround but may work for some deployments.

  2. Configure an additional ACL entry in the inbound access-list to permit the incoming GRE traffic.

ISO CLNS

- CSCek47888

  Symptoms: When a Traffic Engineering (TE) tunnel is configured for IS-IS, a router may resignal the LSPs after the IP routing process is restarted, causing the LSP IDs to be changed.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco ION software image and that functions as a Designated Router (DR) in a LAN when you enter the **process restart iprouting.iosproc** command.

  Workaround: On the router on which the IP routing process is restarted, for each LAN interface on which IS-IS is enabled, enter the **isis priority** *number-value* command, in which the *number-value* argument is 0. Doing so prevents the router from functioning as the DR in the LAN.

- CSCse85158

  Symptoms: Locally advertised networks that are configured for the NSAP address- family under BGP will not be readvertised once they have been cleared from the BGP table.

  Conditions: Once the **clear bgp nsap unicast *** command has been issued, the networks will no longer appear in the output of the **show bgp nsap unicast** command.

  Workaround: There is no workaround.

Miscellaneous

- CSCef73349

  On a Cisco 800 router running inter vrf forwarding between Ethernet0 and Ethernet2, the cef adjacency table might be deleted for entries out of Ethernet0.

  Workaround: .no ip route-cache cef on both ethernet .arp timeout 10 .Static mac

- CSCeg00531

  Symptoms: A router crashes when you remove an ATM subinterface.

  Conditions: This symptom is observed when the subinterface is configured with a LANE client that is configured for Multiprotocol over ATM (MPOA).

  Workaround: There is no workaround.

- CSCeg42877

  Symptoms: PPPoA sessions are not coming up in autovcs after entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command. Tracebacks are reported.

  Conditions: This problem is found only if the QoS parameters are configured via the Radius server.

  Workaround: Configure the QoS parameters through the command line interface (CLI).

- CSCeg86867

  Symptoms: An AAA server does not authenticate.

  Conditions: This symptom is observed on a Cisco platform that functions as an AAA server and that runs Cisco IOS Release 12.3(13) when you dial up using Microsoft callback through an asynchronous line. Dialup through an ISDN modem works fine.

  Workaround: There is no workaround.

- CSCei39688

  Symptom: An ATM PVC configured with OAM on a Cisco Router may fail to pass traffic even when PVC link status is up because of a CEF initialization failure.

```
Router#show ip interface brief | include ATM
ATM3/0/0 unassigned YES manual up up
ATM3/0/0.100 unassigned YES unset up up
ATM3/0/0.300 10.1.1.1 YES manual up up
ATM3/0/0.999 unassigned YES unset up up
Router#show cef interface brief | include
ATM ATM3/0/0 unassigned up dCEF
ATM3/0/0.100 unassigned down dCEF
ATM3/0/0.300 10.1.1.1 down dCEF
ATM3/0/0.999 unassigned down dCEF
Router#show ip cef | include 10.1.1. 10.1.1.0/30 attached ATM3/0/0.300
```

  As CEF fails to initialize the ATM PVC, atm3/0/0.300, no /32 receive entries are created. Traffic destined for the subinterface's IP address is dropped.

  Workaround: Issue "shut" and then "no shut" on the affected ATM subinterface or do not configure OAM on the PVC.

  After the workaround has been applied:

  Router#show ip cef | include 10.1.1. 10.1.1.0/30 attached ATM3/0/0.300 10.1.1.0/32 receive 10.1.1.1/32 receive 10.1.1.3/32 receive

- CSCek36995

  Symptoms: A static 0.0.0.0/0 route is configured with the object tracking feature. The route is then redistributed into RIP. Every 60 seconds, the route is validated and an additional, unnecessary nexthop entry is inserted into the RIP database. The number of these entries will then continue to grow until the route is removed from the database.

  Example:

```
ip route 0.0.0.0 0.0.0.0 FastEthernet0 track 10


router#show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0    redistributed
    [1] via 0.0.0.0,
    [1] via 0.0.0.0,
    [1] via 0.0.0.0,
    [1] via 0.0.0.0,
    [1] via 0.0.0.0,
    [1] via 0.0.0.0,
    [1] via 0.0.0.0
```

  Conditions: This symptom is platform-independent. IP forwarding and routing updates are not affected. Over time, the database will simply grow to an unnecessarily large size. The condition only occurs with the 0.0.0.0/0 route. Other routes are not affected.

  Workaround: Do not use object tracking with the 0.0.0.0/0 route.

- CSCek39470

  Symptom: Cisco IOS router running Cisco IOS Release12.4 may experience per packet memory leak due to pak subblock leak in Process memPool (not in IO mem pool). The symptom is: "show proc mem 1" output seeing the first allocator's memory count is keep growing, and never decrease.

  Condition: The leak is observed with BVI (Bridge-group Virtual Interface) interface configured with crypto ipsec tunnels. Specifically when the router is doing decryption, then send the decrypted packet to BVI interface.

  Workaround: Shut down any BVI (Bridge-group Virtual Interface) if being used in a router with crypto ipsec configured.

- CSCek45344

  Symptoms: A Cisco AS5400XM gateway crashes after 24 hour stress with E1-R2 calls.

  Conditions: This symptom occurs in stress conditions after a period of 24 hours.

  Workaround: There is no workaround.

- CSCek45461

  Symptoms: Path confirmation fails for voice calls on a Cisco AS5850. One-way audio may occur with manual phones.

  Conditions: These symptoms are observed on a Cisco AS5850 that processes MGCP, H.323, and SIP calls.

  Workaround: There is no workaround.

- CSCek46936

  Release-note: Cisco 1700 router hangs or crashes while reloading when configured 56K line speed.

- CSCek50172

  Symptoms: An EEM policy with event interface can not be registered and traceback appears.

  Conditions: This symptom has been observed when configuring the EEM policy with event interface, and specifying a poll-interval larger than 2097151.

  Workaround: When configuring the EEM policy with event interface, specify poll- interval with value less than 2097151.

- CSCek52778

  Symptoms: Dialer idle timer is not reset by interesting traffic on ISDN NON- MLPP, Async MLPPP, Async PBR user sessions.

  Conditions: This symptom is found on a Cisco AS5850 that is running Cisco IOS Release 12.4(7b). Problem may occur with involvement of virtual profiles.

  Workaround: There is no workaround.

- CSCek52801

  Symptoms: Router reloads with corrupted program counter after entering set cos precedence table with longstring under policy-map.

  Workaround: There is no workaround.

- CSCek54481

  Symptoms: HTTP query data is not cached on the HTTP Client.

  Conditions: This symptom has been observed when making voice calls with a VXML script accessing the HTTP Server with query data (a question mark '?' after the URL). The response data from the HTTP Server is not cached on the HTTP Client, which is the Cisco IOS voice brower.

Workaround: Instead of using query (?) to retrieve a file from the HTTP Server, use a static file name with the query character (?).

- CSCek55001

  Symptoms: A router may crash when you enter the **dir /recursive** command.

  Conditions: This symptom is observed on a router that has a Cisco IOS File System (IFS) and occurs only when 40 subdirectories are created. The symptom does not occur when you enter the **dir** command without the **/recursive** keyword.

  Workaround: When more than 40 subdirectories are created, do not use the **dir /recursive** command. Rather, use the **show disk** command.

- CSCin97669

  Symptoms: The standby RP resets continuously because of synchronization failures.

  Conditions: This symptom is observed on a Cisco router when you first perform and OIR of a VIP in which a port adapter is installed that supports both T1 and E1 (for example, a PA-MC-8TE1+ port adapter) and then an SSO switchover occurs.

  Workaround: There is no workaround. You must power-cycle the standby RP to enable it to come up.

- CSCin98932

  Symptom: MDR reload a VIP with "micro reload slot#" can cause VIP crash

  Conditions: VIP on 7500 platform may crash when Warm rebooted with "micro reload slot#" reloaded.

  Workaround: Use "test crash" at VIP console to MDR reload VIP

- CSCir00786

  Symptoms: When you attempt to update the startup configuration from a file but the **boot** commands are incorrect or you are unauthorized to enter the **boot** commands, a boot configuration error message should be displayed, but this does not occur.

  Conditions: This symptom is observed on a Cisco router after the startup configuration has been updated by SNMP.

  Workaround: Perform the following tasks:

  1. Copy the startup configuration to the running configuration.
  2. Copy the running configuration to the startup configuration.
  3. Verify manually that the **boot** commands are indeed correct and use the CLI to update the startup configuration.

- CSCsb13010

  Symptoms: NAT configurations didn’t go through due to insufficient memory.

  Conditions: This behavior was observed on a Cisco 831 router running Cisco IOS Interim Release 12.4(1.2)PI1a and also Interim Release 12.4(2.2)T.

  Workaround: There is no workaround.

- CSCsb24909

  Symptoms: The router crashes when the Cisco IOS reaches AFW_Instance_IsType.

  Conditions: This symptom has been observed on a Cisco AS5350 gateway using Cisco IOS Release 12.3(14)T3.

  Workaround: There is no workaround.

- CSCsc01531

  Symptoms: The router may crash when trying to place more calls in the BACD queue than the configured queue length.

  Conditions: This symptom has been observed when more calls are placed to BACD queue than the configured queue length.

  Workaround: Set the codec under dialpeer to g711ulaw.

- 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.

- CSCsc97398

  Symptoms: The user information Layer 1 protocol may be included in the outgoing bearer capability and may be set to either G711 u-law or G711 A-law. Some PBXs may refuse the call because of this mismatch in the bearer capability.

  Conditions: This symptom is observed when a call is made from H.323 to ISDN with unrestricted digital information bearer capability.

  Workaround: There is no workaround.

- CSCsd28214

  Symptoms: A Cisco router that is running Cisco IOS Release 12.3(19) may crash due to a Watch Dog timeout while running the RIP routing protocol.

  Conditions: The router may crash due to a Watch Dog timeout if an interface changes state at the exact same time a RIP route learned on that interface is being replaced with a better metric redistributed route. For example, RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0. If RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, then the RIP route will be removed. If, during this time the Fast Ethernet 1/0 interface goes down, then the router may potentially crash due to a Watch Dog timeout.

  Workaround: There is no workaround.

- CSCsd40723

  Symptom: When the SESM pushes out new configuration to the ISG, the DHCP clients on dhcp-initiated sessions may not be able to obtain an ip address after the configuration push.

  Conditions: This symptom has been observed when the ISG changes the classname for sessions which were initiated via DHCP.

  Workaround: There is no workaround.

- CSCsd67458

  Symptoms: Dual-tone multifrequency (DTMF) double-digit/garbled digit is heard.

  Conditions: This symptom occurs when a remote call is transferred to a local analog phone, and the DTMF key is depressed from the remote phone.

  Workaround: There is no workaround.

- CSCsd69469

  *Router crashed for packet testcases when show align cli is given

- CSCsd70835

  *Router crashed stress at AFW_TclModule_CleanSubscriptions - Suite 4

- CSCsd80745

  Symptoms: A router that is configured for IPSec and ISAKMP may reload unexpectedly because of a bus error exception that is triggered by an address error exception.

  Conditions: This symptom is observed rarely and can occur under conditions of isakmp negotiation when a new ike sa is being negotiated. The condition is aggravated when low lifetimes are used for ike and ipsec rekeying.

  Workaround: There is no workaround.

- CSCsd85852

  Symptoms: When a PVC is shut down on the remote side, the PVC subinterface on a router transitions from the down state to the up state within one second, but then remains in the down state after the down retry timers expire.

  Conditions: This symptom is observed on a Cisco router that is configured for Operation, Administration, and Maintenance (OAM) and Dynamic Bandwidth Selection (DBS).

  Workaround: There is no workaround.

- CSCsd87358

  Symptoms: A Cisco router may crash when configuring a hierarchical service policy.

  Conditions: This symptom is observed in a Cisco 7200 series router that is running Cisco IOS Release 12.3(6a). At the time of the crash, configuration contained missing keywords causing some of the configuration lines to be rejected and some classes without match statements.

  Workaround: There is no workaround.

- CSCse05642

  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

- CSCse18355

  Symptoms: A Cisco AS5850-ERSC gateway reboots continuously with the message:

  Bundled Rommon and FPGA versions are different from the current system version. Updating the system. This might take a while

System reload is required before upgrade can be done. Rebooting the system .. !

Conditions: This symptom has been observed when a Cisco AS5850-ERSC gateway is running Cisco IOS interim Release 12.4(7.24)T.COMP.

Workaround: Boot to ROM monitor mode and enter the following commands:

SKIP_UPGRADE=1 sync

This step skips the upgrade process. To revert back, enter the following commands:

unset SKIP_UPGRADE sync

- CSCse23478

  Symptoms: A user configured rip routing protocol like this:

  router rip version 2 network ... network ... no auto-summary

  now under a interface it is added:

  interface x/y ip summary-address rip 0.0.0.0 0.0.0.0

  However there is no route to 0.0.0.0/0 in the routing table.

  Under this specific condition the router may generate a spurious memory access or depending on the platform, the router may crash.

  Workaround: Before entering the ip summary router make sure that there is a route to 0.0.0.0/0 in the routing table.

- CSCse28172

  Symptom: RIP routes that point to the dialer interface remain in the routing table when a DSL link goes down. However the routes are removed from the RIP database.

  Conditions: This symptom is observed on a Cisco 877 that runs Cisco IOS Release 12.4(4)T1 or Release 12.4(6)T when the dialer interface is located within a VRF. The symptom is both plaform- and release-independent.

  Workaround: Clear the routing table.

- CSCse28590

  Symptom: Router crashes after entering some map-list commands under global config mode

  Conditions: These commands can cause the crash, but they might not be the only commands would cause such crash:

  ```
  map-list aaaaaaaaaabbbbbbbbbb
  source-addr X121 100
  dest-addr E164 100
  map-list aaaaaaaaaabbbbbbbbbb
  source-addr X121 100
  dest-addr X121 100
  map-list aaaaaaaaaabbbbbbbbbbcccc
  ```

  Workaround: There is no workaround.

- CSCse39191

  Symptoms: A Cisco router that is running DHCP service will run out of memory eventually and will require a reload to recover. You can confirm this by issuing the **show proc mem | inc DHCP** command and seeing that the process named "DHCPD Receive" consumes an increasing amount of memory until the available memory is exhausted.

In addition, the number of AAA sessions will constantly increase and will not decrease when DHCP bindings expire. You can see this by noticing how the output of the **show aaa session** and **show aaa user all** commands show a constantly increasing number of sessions, with those associated with DHCP bindings never vanishing.

Conditions: This symptom has been observed on Cisco routers operating as a DHCP relay or server with one or more DHCP pools configured via the **ip dhcp pool** *name* command where **accounting dhcp** is configured in at least one pool, and the configured poolname is not the name of a valid AAA method list.

This symptom has been observed also when there is very little free processor memory on the router, enabling the allocation of some but not all data structures necessary to perform accounting for a DHCP binding.

Workaround 1: If you do not want AAA accounting for DHCP leases, disable **accounting method** *MethListName* in the DHCP pool by configuring **no accounting method** *MethListName* while in the pool configuration mode.

Workaround 2: If you want AAA accounting for DHCP leases, configure a valid accounting method list by configuring **aaa accounting network methodlistname start-stop method1** where the configured method list name for the accounting method list EXACTLY matches the name provided on the **accounting methodlistname** line in the DHCP pool configuration.

- CSCse40824

  Symptom: router crashes at vxml_uri_compare

  Conditions: This symptom has been observed when the router has been continuously running thousands of scripts loaded thru tftp.

  Workaround: There is no workaround.

- CSCse42444

  Symptoms: When you run and monitor the cbQosCMDropPkt MIB variable, the counters may become stuck while the command line is growing properly. When you run and monitor the cbQosPoliceExceededPkt MIB variable, both counters report the same value.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(15)T13 but may also affect Release 12.4.

  Workaround: There is no workaround.

- CSCse43066

  Symptoms: A Cisco Multiservice IP-to-IP Gateway (IPIPGW) may crash while functioning under stress.

  Conditions: This symptom is observed on a Cisco IPIPGW that runs Cisco IOS interim Release 12.4(9.4) or interim Release 12.4(9.9)T.

  Workaround: Configure slow start:

  voice service voip h323 call start slow

  Note The symptom does not occur in releases earlier than interim Release 12.4(9.4) or interim Release 12.7(7.24)T.

- CSCse48814

  Symptoms: A router crashes when you enter the **ip nat outside** interface configuration command on an interface.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim Release 12.4(9.13) or interim Release 12.4(09.19a) and that is configured for Network Based Application Recognition (NBAR).

Workaround: There is no workaround.

- CSCse50445

  Symptoms: A router that is configured for AutoQoS may crash when the stack for the Exec process is running low.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) or interim Release 12.4(09.19a).

  Workaround: Enter the **ip nbar protocol-discovery** command.

- CSCse50887

  Symptoms: MGCP IOS Gateway sees the following:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  and then:

  ```
  config term router(UNKNOWN-MODE)
  ```

  Or, the **show running-config** command output is only 5 bytes.

  Conditions: This symptom occurs under the following conditions:

  - Use MGCP with the **ccm-manager config** command
  - Have more than 20 MGCP end points (voice ports)
  - Run Cisco IOS Release 12.3(11)T or later releases
  - Reset device pool from Cisco CallManager

  Workaround: Add the **no ccm-manager config** command.

- CSCse55588

  Symptoms: Several Cisco 836 routers crash at least once a day at memcpy with same traceback in YG4.

  Conditions: This symptom has been observed on Cisco 836 routers.

  Workaround: There is no workaround.

- CSCse55652

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

  Conditions: This symptom is observed on a distributed router such as a Cisco AS5850 or Cisco 7500 series that runs Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCse59775

  Symptoms: A Cisco 3845 that is configured for voice may reload because of a software-forced crash that is caused by a Redzone memory corruption.

  Conditions: This symptom is observed on a Cisco 3845 that runs Cisco IOS interim Release 12.4(9.15).

  Workaround: There is no workaround.

- CSCse63494

  Symptoms: A router that is configured for Real-Time Protocol (RTP) may generate CPUHOG events and a traceback similar to the following:

```
%SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
(951/33),process = VOIP_RTCP. -Traceback= 0x60EA5A78 0x60EA5C5C 0x614AD39C 0x614B55BC
0x614B59A0
```

Alternatively, the router may unexpectedly reload and generate the following error message and traceback:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = VOIP_RTCP. -
Traceback= 0x60EA5A58 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0

%Software-forced reload Preparing to dump core...
```

Conditions: This symptom is observed on a Cisco router that receives a badly formatted RTP Control Protocol (RTCP) packet.

Workaround: There is no workaround.

Further Problem Description: Typically, the badly formatted RTCP packet is produced by a device that does not conform to the RFC 3550 standard.

- CSCse64462

  Symptom: A Cisco 7200 series router may encounter a block overrun with Redzone corruption, and subsequently crash if Turbo ACL is configured and the following command is entered:

  clear eou all

  Error messages similar to the following will be output, with associated tracebacks:

  ```
  %SYS-3-OVERRUN: Block overrun at <address> (red zone <value>) %SYS-6-BLKINFO:
  Corrupted redzone blk <address>
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router running Cisco IOS Release 12.4 that is configured for Turbo ACL and when the following command is entered:

  ```
  clear eou all
  ```

  Workaround: Disable Turbo ACL by entering the following command:

  no access-list compiled

- CSCse66112

  Symptom: Configure CFB/MTP on CMM ACT card using the sccp ccm CLI without any version. And add the MTP as the CMM on the call manager administration page.

  Conditions: This symptom has been observed on a CMM running Cisco IOS Release 12.4(8) and on CCM version 5.X.

  Workaround: Register the CFB/MTP with the version included in the SCCP ccm CLI.

- CSCse68065

  Symptom: Memory leakage is detected when malformed SIP packets are sent to Cisco IOS SIP platforms.

  Conditions: SIP (CME, IPIPGW, voice gw) is configured.

  Workaround: There is no workaround.

- 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

- CSCse68355

  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

- CSCse69335

  Symptoms: Media Gateway Control Protocol (MGCP) FXS/FXO port and Cisco IOS T1CAS resets during Hookflash transfer with CCM being the call agent.

  Conditions: This symptom has been observed when two consecutive RQNT messages with S: rel event is received at the Cisco IOS gateway. In this condition, the second RQNT message will not be acknowledged by the Cisco IOS gateway. This results in reset of all the MGCP endpoints on the Cisco IOS gateway.

  Workaround: There is no workaround.

- CSCse71815

  *Router crash when ip VRF forwarding is removed from crypto outside intf

- CSCse73517

  Symptom: When a Cisco 2821 is configured with ’warm-reboot count 3’ and when it tries to boot Cisco IOS Release 12.4(9.9) or 12.4(9.10) or 12.4(9.12), it will fail and stuck in "Emulating mis-aligned store" loop.

  Conditions: Cisco IOS Release 12.4(8) does not have this problem, but the problem starts from Release 12.4(9.9).

  Workaround: Remove ’warm-reboot count 3’ from the configurations.

- CSCse75920

  Symptoms: A Cisco router experiences a memory leak for the processes SCCP application and Chunk manager.

  Conditions: The symptom has been observed after configuring the router for MTP and transcoding.

  Workaround: There is no workaround.

- CSCse79884

  Symptoms: You may not be able to exit the **session** command.

  Conditions: This symptom is observed on MWAM line card processors that are installed in a Cisco Catalyst 6500 series switch or a Cisco 7600 series router.

  Workaround: If the **session** command is executed via a Telnet session to the supervisor engine: log in to the supervisor engine via its console to find out the line number in the output of the **show user** command that corresponds to the processor that is unable to exit from the **session** command. Look for IP address 127.0.0. <slot> <processor number used for session> to find the line number. Then, enter the **clear line** *line number* command to clear the session.

  If the **session** command is executed from the MWAM console itself (which is stuck), there is no workaround.

- CSCse82487

  Symptom: Router crashes and emits Traceback at config_ip_keyswitch_dp_pattern.

  Conditions: While issuing the command "dialplan-pattern 5 aaaaaaaaaabbbbbbbbbbccccccccccddddddddddeeeeeeeeeeffffffffffgggggggggghhhhhhhhhhiiiiiiiiiij jjjjj
  jjjjkkkkkkkkkkllllllllllmmmmmmmmmmnnnnnnnnnnoooooooooopppppppppppqqqqqqqqqqrrrrrrrrrrs extension-length 32 extension-pattern string2 no-reg"

  Workaround: There is no workaround.

- CSCse85329

  Symptoms: When you re-insert a PA-MC-8TE1+ port adapter in the same slot of a Cisco 7200 series via an OIR, the serial interface may enter the Down/Down state. When you enter the **shutdown** command followed by the **no shutdown** command on the T1 or E1 controller, the serial interface may transition to the Up/Down state, still preventing traffic from passing.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(7) or a later release.

  Workaround: Reload the router.

- CSCse87017

  Symptom: Cisco IOS H.323 gateway may disconnect a transfer from 3rd party H.323 gateways after generating the an error message similar to the one below: %VOICE_IEC-3-GW: H323: Internal Error (Software Error): IEC=1.1.180.5.13.36 on callID 111

  Conditions: Observed on 3845 running Cisco IOS Release 12.4Mainline and Cisco IOS Release 12.4T release

  Workaround: There is no workaround.

- CSCse88031

  Symptom: User may be unable to add an uplink interface to an "ssg direction uplink member" group.

  Conditions: 2821/2xVWIC2-2MFT-T1/E1 running c2800nm-advipservicesk9-mz.124-9.T

Issue seems to happen during an initial configuration of SSG global commands and may trigger when configuring global "ssg bind service" commands before interface "ssg direction uplink member" commands.

Workaround:

1. Configure 'ssg direction uplink member' interface commands before global 'ssg bind service' commands.
2. 'default interface ser0/1/1:0' followed by a router reload which then allows 'ssg direction uplink member' to be configured on new serial interface.

- CSCse88516

  Symptom: When testing Cisco IOS Release 12.4(9.15)T image, found CLI setting for jitter buffer playout delay Minimum doesn't work. Was able to set to 10ms with "playout-delay minimum low" on voip dial- peer, but debug shows it use 40ms.

  Test topology:

  ```
  analog phone---OGW(2800)---- VoIP(H.323)---TGW(2800)---Analog phone.
  ```

  Conditions: It happened on palyout-delay mode setting is adaptive (default), not to fixed mode.

  Configuration in Gateway: OGW:

  ```
  dial-peer voice 1004 voip destination-pattern 1004 session target ipv4:1.1.2.199
  playout-delay minimum low codec g711ulaw
  ```

  ```
  TGW:
  ```

  ```
  dial-peer voice 1004 voip incoming called-number 1004 playout-delay minimum low codec
  g711ulaw
  ```

  ```
  dial-peer voice 91000 pots destination-pattern 10.. port 1/0/0
  ```

  Workaround: Use playout-delay mode fixed to get jitter buffer playout delay Minimum 10ms.

- CSCse89105

  Symptoms: RADIUS packets may be dropped or extra memory may be allocated when RADIUS packets are sent.

  Conditions: These symptoms are observed on a Cisco platform that is configured for SSG when a RADIUS packet with a length of more than 1024 bytes is sent.

  Workaround: There is no workaround.

- CSCse89373

  Symptoms: A second PRI link gets deactivated, with no ability to process incoming and outgoing calls, when the second one is remotely, physically, manually (CLI command) deactivated.

  Conditions: This symptom occurs when the first PRI is type primary-net5, and the second PRI is type primary-qsig. Deactivate the second PRI remotely or locally by physically disconnecting the cable or issuing the **shutdown** command under the corresponding E1 controller.

  Workaround: There is no workaround.

- CSCse89402

  Symptoms: The CPU stack frame may become corrupted when a channel-group is configured on the T1/E1 controller.

  Conditions: This symptom is seen on mainboard WIC slots when the slot is configured for the "no network-clock participate."

  Workaround: Use the VWIC in "network-clock participate" when installed in the mainboard WIC slot of the router.

Further Problem Description: In most situations, no problems are seen. In rare cases, a crash may occur.

- CSCse90702

  Symptoms: A Frame Relay map may not be established after you perform an OIR of a line card.

  Conditions: This symptom is observed on a Cisco 7600 series when the line card is configured with an MFR bundle.

  Workaround: Create a static Frame Relay map.

  Alternate Workaround: Perform an OIR at both ends simultaneously.

- CSCse91102

  Symptoms: A Cisco IAD 2430 IAD crashes on Cisco IOS Release 12.4(4)T2. Traceback decodes indicate memory corruption. The following events may also appear in the log:

  ```
  %SYS-3-BADMAGIC: Corrupt block at %SYS-6-MTRACE: mallocfree: addr, pc %SYS-6-BLKINFO:
  Corrupted magic value in in-use block %SYS-6-MEMDUMP:
  ```

  Conditions: The router crashes where the decodes indicate check heaps as the source with any or all of the following also included in decode:

  crashdump validblock validate_memory checkheaps checkheaps_process

  Workaround: There is no workaround.

- CSCse93156

  Symptoms: IP route configurations, when configured, are not getting visible on the running and startup configurations. CMTS is accepting the IP route configuration, and also the **show ip route** command is getting updated with configured routes.

  Conditions: The symptom occurs while configuring static route. The configured route will not get visible on running and startup configurations.

  Workaround: There is no workaround.

- CSCse93695

  Symptoms: Three-way calls that involve the Broadsoft SIP server and Cisco IAD2400 series Integrated Access Devices may not work.

  Conditions: This problem is observed in Cisco IOS Release 12.4(9)T.

  Workaround: There is no workaround.

- CSCse97112

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

  Conditions: This symptom is observed after the following command is issued:

  no x25 map compressedtcp a.d.c.d ip e.f.g.h [**options**]

  This may cause an Address Error (load or instruction fetch) exception, CPU signal 10.

  Workaround: There is no workaround.

- CSCsf03530

  Symptoms: A crash occurs on a router when it receives a message waiting indicator (MWI).

  Conditions: This symptom is observed when unity sends a notify to the gateway (GW), and the GW is suppose to convert to QSIG MWI. The GW crashes while running Cisco IOS Interim 12.4(9.18)T.

  Workaround: There is no workaround.

- CSCsf03566

  Symptoms: Software-forced crash (SFC) occurs due to memory corruption.

  Conditions: The crash has been seen on a Cisco 7600 router running Cisco IOS Release 12.2(18)SXF5. This happens if the router is acting as an EZVPN sever and xauth is enabled when the crypto session is brought down.

  Workaround: There is no workaround.

- 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

- CSCsf06386

  Symptom: A device running Cisco IOS may leak buffers in I/O memory. Overtime this will exhaust all of I/O memory and can prevent non-console access to the device.

  Conditions: The device must be configured for SSG (Service Selection Gateway)

  Workaround: There is no workaround.

- CSCsf09186

  Symptoms: When you enter the **show ip route** command to check on the installed routes, the output does not show the routes that have been installed by the RIP.

  Conditions: This symptom is observed on a Cisco router when redistribution is enabled under the RIP.

  Workaround: There is no workaround.

- CSCsf09338

  Symptoms: The calls coming from the CMM MTP has one-way audio when a call transfer is done on the other side.

  Conditions: This symptom is observed when CMM is configured as MTP/XCode and running Cisco IOS Release 12.4(7b).

  Workaround: There is no workaround.

- CSCsf11937

  Symptoms: When you enter the **cd .../.../** command followed by a sequence of **mkdir** commands, the disk becomes corrupt.

  Note that for the **cd .../.../** command, ".../.../" are the arguments, that is, the arguments consist of more than two dots.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

Workaround: Enter the **format** command for the file system.

- CSCsf11982

  Symptoms: Cisco 7200 router will crash with ip sla monitor schedule configuration with Cisco IOS Release 12.4(10.5) release.

  Conditions: The router will crash after issuing the below configuration:

  ```
  config terminal ip sla monitor 1 type voip delay post-dial detect-point alert-ringing
  destination 8765432 end
  ```

  ```
  config terminal ip sla monitor schedule 1 life 300 start-time now
  ```

  Workaround: There is no workaround.

- CSCsf12037

  Symptoms: An SNA Switch router may reload and display the following error message:

  System returned to ROM by bus error at PC 0x61504EB0, address 0x58

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.3(18).

  Workaround: There is no workaround.

- CSCsf13740

  Symptoms: A Cisco 7200 series router with VAM2+ Encryption/Compression engine, running Cisco IOS Release 12.4(10), may reload due to a bus error after a large service policy is applied to a Gig interface.

  The following error messages may flood the console:

  ```
  *crypto qos: get_shape_class fail, class=<name>
  ```

  ```
  *crypto qos: get_shape_class fail, class=<name>
  ```

  ```
  *crypto qos: get_shape_class fail, class=<name>
  ```

  ```
  *crypto qos: get_shape_class fail, class=<name>
  ```

  ```
  Crash: %ALIGN-1-FATAL: Corrupted program counter 06:30:27 MEST Fri Aug 18 2006
  pc=0x7E000000 , ra=0x6633E958 , sp=0x64DE2E40
  ```

  ```
  %ALIGN-1-FATAL: Corrupted program counter 06:30:27 MEST Fri Aug 18 2006 pc=0x7E000000
  , ra=0x6633E958 , sp=0x64DE2E40
  ```

  ```
  06:30:27 MEST Fri Aug 18 2006: TLB (load or instruction fetch) exception, CPU signal
  10, PC = 0x7E000000
  ```

  ```
  -Traceback= 0x7E000000 $0 : 00000000, AT : 63F00000, v0 : 00000001, v1 : 64DE2F90 a0
  : 00000000, a1 : 663004BC, a2 : 00000188, a3 : 6454B6D0 t0 : 66419DD8, t1 : 661BFC08,
  t2 : 00000018, t3 : 00000000 t4 : 6410AD00, t5 : 00000001, t6 : 00000000, t7 : 00000000
  s0 : 661BFE50, s1 : 66300940, s2 : 00000A61, s3 : 66302AC4 s4 : 6454AA3C, s5 :
  618D9FF0, s6 : 663003A4, s7 : 63CA0000 t8 : 00000061, t9 : 6410AD00, k0 : 6571911C,
  k1 : 6080F4E4 gp : 63F0AA08, sp : 64DE2E40, s8 : 00000001, ra : 6633E958 EPC :
  7E000000, ErrorEPC : BFC018D4, SREG : 3400FF03 MDLO : 00374C80, MDHI : 00000000,
  BadVaddr : 7E000000 Cause 00000008 (Code 0x2):
  ```

  ```
  TLB (load or instruction fetch) exception Process watchdog registers: $0 : 658FC0EC,
  AT : 00000000, v0 : 606CCE5C, v1 : 00000001 a0 : 658F9E6C, a1 : 00000000, a2 :
  00000000, a3 : 658F6118 t0 : 00000000, t1 : 658FC0B8, t2 : 658FC0EC, t3 : 00000000 t4
  : FFFFFFF7, t5 : 6080F4CC, t6 : 62B23BA8, t7 : 00000001 s0 : 00000000, s1 : 658F9E98,
  s2 : 6543A190, s3 : 00000018 s4 : 6543A190, s5 : 6643D788, s6 : 6497AA80, s7 : 6080F5A0
  t8 : 662F5D6C, t9 : 00000001, k0 : 00000000, k1 : 658FC0B8 gp : 6497AA80, sp :
  00000001, s8 : 658FC0EC, ra : 00000000 EPC : 658FC0B8, SP : 00000001, forkx : 00000000
  ```

  Conditions: This symptom occurs when the router has a VAM+ encryption module.

  Workaround: There is no workaround.

- CSCsf17039

  Symptoms: A router may crash when you configure On-Demand Address Pools (ODAP) with Dynamic Host Configuration Protocol (DHCP) and when the router that requests the address pool (subnet) runs out of available addresses.

  Conditions: This symptom is observed in an MPLS-VPN network when you configure ODAPs on virtual home gateways (VHGs) and provider edge (PE) routers.

  Workaround: There is no workaround.

- CSCsf19418

  Symptoms: A router may reload unexpectedly when you enter the **show mpls ldp graceful-restart** command.

  Conditions: This symptom is observed when either of the following conditions are present:

  - When the command output has a "Down Neighbor Database" entry that expires by reaching the reconnect timeout limit while the command output is generating the neighbor address list.
  - When the command output is paged at the "--More--" string within the context of displaying addresses.

  Workaround: Do not enter the **show mpls ldp graceful-restart** command when a graceful-restart database entry is about to expire. When the command output is paged at the "--More--" string within the context of displaying addresses and when the Down Neighbor Database entry may have expired, type the letter "Q" to abort any further output of addresses.

- CSCsf19728

  A new NextPort firmware needs to be bundled into Cisco IOS to address critical customer issues.

  The firmware has two components: Module Controller Firmware, and SPE Firmware.

  The MC firmware change allows a configurable change to facilitate Modem Pass Through for a specific POS client device, critical to a specific customer.

  The SPE firmware is 10.4.1, and the associated fixes are listed in release notes located at:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/nxtprtrn/

- CSCsf22493

  Symptoms: The Cisco Communication Media Module (CMM) crashes when processing the UnsubscribeDtmf message.

  Conditions: This symptom is observed when CMM XCODE/MTP is using Cisco IOS Release 12.4(8a) and RFC2833.

  Workaround: There is no workaround.

- CSCsf26617

  Symptom: MGCP gateway will intermittently unregister from CallManager when calls to EVM FXS port are being made.

  Conditions: MGCP gateway using EVM module with FXS port. A call is made to the FXS port and the Calling Party hangs up right away. The FXS called party then answers the call during the first ring.

  Since the Calling party hangs up right away the CallManager will continue to send DLCX to the gateway. The gateway will not respond to three DLCXs and the CallManager will unregister the gateway.

  Workaround:

  - Configure the EVM FXS ports to be H.323.

  - Use the vwic on the motherboard instead of the EVM

- CSCsf27178

  Symptom: Percentage based traffic shaping is not working.

  Conditions: This symptom is observed on a Cisco router that is configured the percentage based traffic shaping an output policy

  Workaround: There is no workaround.

- 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

- CSCsf31178

  Symptoms: HWIC-1GE-SFP may experience an issue where the Gig Ethernet interface is "stuck" in a Line UP/Protocol Down state. While in this state, the interface will not pass traffic. Clearing the interface or manually disabling/enabling will clear the condition. This symptom does not occur when 1000BASE-T SFP is used.

  Conditions: A Loss of Signal (for example, unplugging the cable) may cause the interface to become stuck in a Line UP/Protocol Down state.

  Workaround: Clearing the interface or manually shutting it down, then bringing it back up will clear the problem.

- CSCsf97785

  Symptom: eRSC got hung while bootup

  Conditions: This symptom has been observed during bootup.

  Workaround: There is no workaround.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsf98608

  Symptom: GK reloads when "no zone prefix SFO-GK-1 201201* gw-priority 10 SFO_trunk8_8 SFO_trunk6_6 SFO_trunk4_4 SFO_trunk2_2" command is issued on the Gatekeeper.

  Conditions: This symptom has been observed when dynamic prefixes are used.

  Workaround: There is no workaround.

- CSCsf99378

  Symptom: No form of "ip local pool poolname" is not accepted. Error message says it is an incomplete command.

  Conditions: This symptom has been observed on Cisco IOS Release 12.4(10.8) image.

  Workaround: There is no workaround.

- CSCsg00602

  Symptoms: A Cisco 3845 or Cisco 3825 router with AIM-VPN/HPII-PLUS(EPII-PLUS) may show the following symptoms:

  1. Show alignment errors.
  2. Crash by bus error.
  3. XXX display by running the **show crypto engine accel ring packet** command.
  4. If a telnet session, which shows symptom three, is cut by "clear line," its related exec process does not disappear and starts to occupy CPU.

  Conditions: This failure is seen on the Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco 1800 series routers that are configured with an AIM-VPNII or AIM-VPNII PLUS Virtual Private Network (VPN) encryption and hardware advanced integration module (AIM).

  Workaround: Avoid running the **show crypto engine accel ring packet** command.

- CSCsg03991

  Symptoms: * build broke for snasw images

  Workaround: There is no workaround.

- CSCsg05140

  Symptom: A Cisco AS5850 reloads unexpectedly during stress with sip calls.

  Conditions: This symptom has been observed on Cisco AS5850 platform for plain SIP calls.

  Workaround: There is no workaround.

- CSCsg07907

  Symptoms: A Cisco 3845 router unexpectedly reloads with bus error as seen in the show version when enabling DSP mini logger (voice dsp <slot> command history enable).

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4 with conferencing enabled on the DSP slot that minilogger is being turned on for.

  Workaround: Disable conferencing on that slot, if possible.

- CSCsg15598

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.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

- CSCsd71318

  Symptoms: A Cisco 2800 series router crashes whenever the connection to the URL filter server is reset due to network congestion or a warm or cold reload.

  Conditions: This symptom has been observed when the router is running URL filtering with an external Websense or N2H2 server.

  Workaround: There is no workaround for cold or warm reload. If the crash occurs due to network congestion or WAN reset, remove the condition that cause the connection to the URL filter to flap.

Wide-Area Networking

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP.

  Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCir00712

  Symptoms: On Cisco LAC software running Cisco IOS Release 12.3(14)T, when the fragmented data traffic is received on the LAC over the L2TP tunnel, the IP layer reassembles the packet and routes the packet on the wrong interface instead of consuming the L2TP data traffic locally.

  Conditions: This symptom has been seen when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel.

  Workaround: There is no workaround.

- CSCsd75854

  Symptoms: A router may generate a malformed PPPoE Active Discovery Offer (PADO) packet with two 802.1q tags. The first 802.1q tag contains the correct VLAN ID.

  Conditions: This symptom is observed on a Cisco router when the Service-Name field in the PPPoE Active Discovery Initiation (PADI) packet is empty and not equal to the one that is configured on the router.

Workaround: Ensure that a correct Service-Name field in used in the PADI packet.

- CSCsd93740

  Symptoms: A Cisco router is acting as a X25 switch. Both standard X25 route statements and hunt-groups are being used.

  After a period of normal operations, output of the **show x25 hunt- group** command shows status full for all hunt-groups where destinations are reachable over XoT.

  Other hunt groups where calls are forwarded over X25 serial interfaces do not show this problem. When problem is present, calls cannot be forwarded via hunt groups, and configured redundant routes are used.

  Workaround: Unconfigure/configure back all X25 routes helps to recover in some cases. However, in some cases router reload is needed.

- CSCse12198

  Symptoms: Individual B-channels on the primary T1 in the NFAS group sometimes go OOS for no reason.

  Conditions: This symptom is observed when connected to a Cisco PGW that is running Cisco IOS Release 9.3(2). The Cisco AS5400 is connected to the Cisco PGW that is running RLM in the Signaling/Nailed mode.

  Also, sometimes ISDN service goes OOS, and also channel states goes to 5 which is maintenance pending.

  Workaround: When this happens, put ISDN service can be put back in service manually for individual CIC, but channel state cannot manually be put back in service unless the whole serial interface is bounced. This cannot be done when there is other traffic on the other b-channels.

- CSCse34162

  Symptoms: A Cisco router hangs after 5 to 10 minutes of passing traffic over a dialer interface.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 12.4(8) with PPP Multilink configured on a dialer interface and traffic is passing.

  Workaround: There is no workaround. A reboot is required to recover.

- CSCse55872

  A router running Cisco IOS Release 12.3 or later may reload when a "default forwarding group <n>" command is entered.

  Workaround: There is no workaround.

- CSCse78652

  Symptoms: The queuing mode on Multilink interfaces is erroneously defaulting to fair queuing instead of FIFO. This is causing distributed Cisco Express Forwarding (dCEF) to fail on Cisco 7500 routers.

  Conditions: This symptom happens on all Multilink interfaces.

  Workaround: There is no workaround.

- CSCse79994

  Symptoms: BRI Layer 2 remains in the ESTABLISH_AWAITING_TEI state instead of entering the MULTIPLE_FRAME_ESTABLISHED state.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

- CSCse81069

  Symptoms: Unconfiguring the **isdn service b_channel** command is not taking effect. The command is not removed from the running configuration.

  Conditions: This symptom occurs when configuring the **isdn service b_channel** command to a state other than the default value of 0 on the ISDN D channel.

  Workaround: To remove the command, shut down the T1/E1 controller first and then unconfigure the command under the D channel serial interface.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf03251

  Symptoms: Primary and backup NFAS interfaces may transition from WAIT to OOS even after receiving "in-service" message from the PSTN.

  Conditions: This symptom is observed on a Cisco AS5400XM that is running several Cisco IOS Release 12.4 mainline and Release 12.4T.

  Workaround: There is no workaround.

- CSCsf28839

  Symptoms: When you change the encapsulation from Frame Relay to another type, a spurious memory access and tracebacks are generated.

  Conditions: This symptom is observed on a Cisco router that has the **encapsulation frame-relay** command enabled on a serial interface when you assign the serial interface to an MFR interface, which causes the Frame Relay encapsulation to be removed from the serial interface.

  Workaround: There is no workaround.

- CSCsg15642

  Symptoms: A PSTN Gateway unexpectedly restarts due to a lack of memory. Overtime memory utilization increases, and the **show processes memory sorted** command indicates that the ISDN process is allocating an increased amount of memory.

  Conditions: This leak occurs when a SETUP message with Display IE is received.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(10c)

Cisco IOS Release 12.4(10c) is a rebuild release for Cisco IOS Release 12.4(10). The caveats in this section are resolved in Cisco IOS Release 12.4(10c) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsg21398

  Symptoms: The Cisco IOS software image may unexpectedly restart when a crafted “msg-auth-response-get-user” TACACS+ packet is received.

Conditions: This symptom is observed after the Cisco platform had send an initial “recv-auth-start” TACACS+ packet.

Workaround: There is no workaround.

- 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 “%DATACORR UPTION-1-DATAINCONSISTENCY” message and note those to your support contact.

IP Routing Protocols

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- CSCek47667

  Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

  Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsg00860

  Symptoms: Enabling NAT outside on the public interface terminates the VPN connection as GREoverIPSEC. Inbound ACL applied on the public interface starts to drop decrypted GRE traffic.

  Conditions: This symptom has been observed with the use of IP NAT outside on the public VPN interface.

  Workaround: There are 2 workarounds:

  1. Configure NAT translations for all traffic, to force NAT processing on the packet even if no address will actually be translated. Example:

  ip nat inside source static 172.16.68.5 172.16.68.5

  It is not a scalable workaround but may work for some deployments.

  2. Configure an additional ACL entry in the inbound access-list to permit the incoming GRE traffic.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh80678

  Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(22) or a later release when the **auto-summary** command is enabled for BGP.

  Workaround: Enter the **no auto-summary** command.

- CSCsh90153

  Symptoms: Connectivity is lost through a router when traffic is processed twice by NAT.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(8a), that is configured for NAT and PBR, and that has a firewall feature enabled. Under certain conditions, traffic is processed twice by NAT when it does not need to be.

  Workaround: Remove the firewall configuration from the router.

  Further Problem Description: Syslogs and the output of the **show ip nat translation** command show that traffic that is processed twice by NAT does not traverse the router.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

  Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  Workaround: Add area 0 in the OSPF VRF processes.

  Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

Miscellaneous

- CSCds25257

  Symptoms: A gatekeeper rejects new registration requests from a Cisco Unified CallManager (CUCM) or other H.323 endpoints with Registration Rejection (RRJ) reason of duplicateAlias. Attempting to clear this stale registration fails and a “No such local endpoint is registered, clear failed.” error message is generated.

  Conditions: This symptom is observed in the following topology:

  CUCM H.225 trunks register to a gatekeeper (GK) cluster. Gatekeeper 1 (GK1) and gatekeeper 2 (GK2) are members of the GK cluster. The CUCM registers first to GK1, then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

  When the H.225 trunk attempts to register with GK1, it is rejected because the alternate registration is still present, and there is no way to clear it.

```
10.9.20.3       34273 10.9.20.3       32853 SJC-LMPVA-GK-1    H323-GW A
    ENDPOINT-ID: 450FC24400000000  VERSION: 5  AGE: 1618993 secs
SupportsAnnexE: FALSE
    g_supp_prots: 0x00000050
    H323-ID: SJC-LMPVA-Trunk_4
```

  Workaround: Reset the gatekeeper by entering the **shutdown** command followed by the **no shutdown** command, or reboot the affected GK.

- CSCek38201

  Symptoms: A router may reload or display an alignment traceback when you enter the **show crypto socket** command.

Conditions: This symptom is observed on a Cisco router that has an OSPFv3 IPSecv6 configuration.

Workaround: There is no workaround. To prevent the symptom from occurring, do not enter the **show crypto socket** command in an OSPFv3 IPSecv6 configuration.

- CSCek45344

  Symptoms: A Cisco AS5400XM gateway crashes after 24 hour stress with E1-R2 calls.

  Conditions: This symptom occurs in stress conditions after a period of 24 hours.

  Workaround: There is no workaround.

- CSCek64789

  Symptoms: A router that is configured as a voice gateway may crash because of a bus error. Just before the crash occurs, messages of the following type may be generated:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  ```

  Conditions: This symptom is observed on a Cisco 2811 that is configured as a Cisco Multiservice IP-to-IP Gateway (IPIPGW). However, the symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCsd28214

  Symptoms: A Cisco router may crash because of a watch dog timeout while running the RIP routing protocol.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3(19) when an interface changes state at the exact same time that a RIP route that was learned on this interface is being replaced with a better metric redistributed route. For example, when RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0 interface and then RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, the RIP route is removed. However, when during this time the Fast Ethernet 1/0 interface goes down, the router may crash because of a watch dog timeout. Note that the symptom may also affect other releases.

  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

- 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.

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- CSCse91102

  Symptoms: A Cisco IAD 2430 IAD crashes on Cisco IOS Release 12.4(4)T2. Traceback decodes indicate memory corruption. The following events may also appear in the log:

  ```
  %SYS-3-BADMAGIC: Corrupt block at
  %SYS-6-MTRACE: mallocfree: addr, pc
  %SYS-6-BLKINFO: Corrupted magic value in in-use block
  %SYS-6-MEMDUMP:
  ```

  Conditions: The router crashes where the decodes indicate check heaps as the source with any or all of the following also included in decode:

  ```
  crashdump
  validblock
  validate_memory
  checkheaps
  checkheaps_process
  ```

  Workaround: There is no workaround.

- CSCsg08395

  Symptoms: When one of the controllers of a VWIC-2MFT-E1 Voice/WAN interface card that is connected back-to-back to another router is shut down, ISDN L2 may go down on the second E1 controller of the VWIC-2MFT-E1.

  Conditions: This symptom is observed on a Cisco 3725 that runs Cisco IOS interim Release 12.4(11.1).

  Workaround: There is no workaround.

- 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.

- CSCsg59326

  Symptoms: When an ATM (that is, a cash machine, not a WAN platform) is connected to a switch service module, significant packet loss may occur.

  Conditions: This symptom is observed on a Cisco 2800 series router.

  Workaround: Change the Ethernet speed to 10 Mbps at both ends.

- 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

- CSCsg96319

  Symptoms: When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:***number ip-address* command.

  Conditions: This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhanmt_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  Workaround: Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- CSCsg99814

  Symptoms: On a router that functions in a GRE over IPSec or Virtual Tunnel Interface (VTI) configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface.

  Conditions: This symptom is observed when the ACL on the tunnel interface is configured on the outbound physical interface on which the IPSec tunnel is terminated.

Workaround: Apply the outbound ACL on the protected LAN interface instead of on the tunnel interface.

- CSCsh33430

  Symptoms: A traceback may occur in an HSRP function and the platform may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that has the HSRP Support for ICMP Redirects feature enabled and occurs when a learned HSRP group is removed after a resign message has been received.

  Workaround: Disable the Support for ICMP Redirects feature by entering the **no standby redirects** global configuration command.

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

  ```
  %MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of
  [dec] - VRF [chars]
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

  Workaround: There is no workaround.

- CSCsh58082

  Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

  There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

  Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsh75827

  Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the “J” Service-Info attribute), has logged out from the SESM, and then renews its IP address.

  Workaround: There is no workaround.

- CSCsh92914

  Symptoms: A router may unexpectedly reload when you attempt to open a reversed SSH connection by using the SSHv1 protocol.

  Conditions: This condition is observed on a Cisco router that runs Cisco IOS Release 12.4.

  Workaround: Force the SSH transport to be SSHv2 by entering the **ip ssh version 2** global configuration command.

- CSCsh94526

  Symptoms: When an acct-stop message is received for a non-RADIUS proxy user (that is, a normal IP user), a router that is configured for SSG crashes.

  Conditions: This symptom is observed when SSG is configured for RADIUS proxy mode and when the **ssg wlan reconnect** command is enabled.

  Workaround: There is no workaround.

- CSCsh97579

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi27540

  Symptoms: A VSI session may become stuck in the “RESYNC_UNDERWAY” state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

  Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

  Workaround: There is no workaround.

- 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

- CSCsi67763

  The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

  http://www.kb.cert.org/vuls/id/739224

  By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

  Cisco response is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml

- CSCsi84017

  Symptoms: When you reload a Cisco 2600 series, the router may hang.

  Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek60025

  Symptoms: A ping may be dropped in a PPP callback scenario.

  Conditions: This symptom is observed on a Cisco router when Multilink PPP (MLP) and the **dialer load-threshold** command are enabled.

  Workaround: There is no workaround.

- CSCsc39890

  Symptoms: A router that is running Cisco IOS may reload unexpectedly.

  Conditions: For this symptom to occur, the router must be configured for ISDN. One possible trigger is when using SNMP to poll information about calls while the calls are in the process of completing.

  Workaround: There is no workaround.

- CSCsf30493

  Symptoms: When a T.37 onramp call is made, the following error message may be generated:

  ```
  %CSM-3-NO_VDEV: No modems associated
  ```

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS interim Release 12.4(10.7). The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsh06841

  Symptoms: A router may crash while establishing a PPP session.

  Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

  Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsh82513

  Symptoms: The output of the **show isdn active** command may show disconnected calls.

  Conditions: This symptom is observed on a Cisco router when analog modem calls are made after a normal ISDN digital call has been made.

  Workaround: There is no workaround.

- CSCsi21853

  Symptoms: When you attempt to change the ISDN T306 timers, the changes are not accepted.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4. The symptom may also affect Release 12.4T.

  Workaround: There is no workaround.

  Further Problem Description: The ISDN T306 configuration updates the values of the ISDN T307 timers.

- CSCsi74960

  Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

  Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

  Workaround: There is no workaround.

- CSCsj10593

  Symptoms: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(15.6) and that functions as a TGW with all PRI switch types from the user to the network side. The symptom occurs when the **isdn test call interf ace** *interface-number dialing-string* command is entered at the platform on which the call is initiated, when the originating gateway (OGW) is configured for the National ISDN (primary-ni) switch type, and when the TGW is configured for the NT DMS-100 (primary-dms100) switch type. The symptom may also affect Release 12.4T.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(10b)

Cisco IOS Release 12.4(10b) is a rebuild release for Cisco IOS Release 12.4(10). The caveats in this section are resolved in Cisco IOS Release 12.4(10b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsf32390

  Symptoms: When tuning particle clone, F/S, and header pools after these were made configurable via CSCuk47328, the commands may be lost on a reload.

  Conditions: If the device is reloaded the commands are not parsed on a reload and this results in the defaults being active. This may result in traffic loss if the increased buffers were needed to enable greater forwarding performance for the specific network design.

Workaround: Configure an applet to enter the buffer values again after a reload. A sample applet would be:

```
event manager applet add-buffer
 event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "buffers particle-clone 16384"
 action 4.0 cli command "buffers header 4096"
 action 5.0 cli command "buffers fastswitching 8192"
 action 6.0 syslog msg "Reinstated buffers command"
```

- CSCsg03830

  Symptoms: The **tacacs-server directed-request** command appears in the running configuration when is should be disabled. When you disable the command by entering **no tacacs-server directed-request** and reload the router, the command appears to be enabled once more.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for CSCsa45148, which disables the **tacacs-server directed-request** command by default.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa45148. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Temporary Workaround: Each time after you have reloaded the router, disable the command by entering **no tacacs-server directed-request**.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  – You reload the router.

  – A switchover of the active RP occurs.

  – You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. Is this not an option, there is no workaround.

Interfaces and Bridging

- CSCsg64182

  Symptoms: VIP may crash due to a bus error.

  Conditions: This symptom occurs when a dot1q subinterface on the VIP is configured with a service policy.

  Workaround: Remove the service policy.

IP Routing Protocols

- CSCsf27220

  Symptoms: A Cisco 7500 series router with any ATM Port Adapter may crash.

  Conditions: This symptom is observed when a router is configured with the Next Hop Resolution Protocol (NHRP) feature. When sending traffic, the router will crash.

  Workaround: There is no workaround.

Miscellaneous

- CSCed57504

  Symptoms: A router reloads when a session using virtual-template configuration and terminated on this router is being cleared from the DSL CPE router that is the peer router for the connection.

  Conditions: This symptom occurs when a session using virtual-template configuration and terminated on this router is being cleared from the DSL CPE router that is the peer router for the connection.

  Workaround: There is no workaround.

- CSCei39688

  Symptoms: When a CEF initialization failure occurs, an ATM PVC that is configured for OAM may not pass traffic even though the PVC link status is up:

```
Router#show ip interface brief | include ATM
ATM3/0/0                   unassigned      YES manual up      up
ATM3/0/0.100               unassigned      YES unset  up      up
ATM3/0/0.300               10.1.1.1        YES manual up      up
ATM3/0/0.999               unassigned      YES unset  up      up

Router#show cef interface brief | include ATM
ATM3/0/0                        unassigned      up      dCEF
ATM3/0/0.100                    unassigned      down    dCEF
ATM3/0/0.300                    10.1.1.1        down    dCEF
ATM3/0/0.999                    unassigned      down    dCEF

Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
```

When CEF fails to initialize the ATM PVC, atm3/0/0.300, no /32 receive entries are created. Traffic that is destined for the IP address of the subinterface is dropped.

Conditions: This symptom is observed on a Cisco router and occurs only when PAM is configured on the PVC.

Workaround: To prevent the symptom from occurring, do not configure OAM on the PVC. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM subinterface. After the workaround has been applied, the output of the **show ip cef** command shows the following:

```
Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
10.1.1.0/32     receive
10.1.1.1/32     receive
10.1.1.3/32     receive
```

- CSCek48251

  Symptoms: When you enter the **redundancy switch-activity force** command on the active eRSC of a Cisco AS5850 while incoming VoIP H.323 calls and outgoing CAS calls are being processed, the standby eRSC does become the active eRSC and processes the calls but soon afterwards may crash at "csm_enter_idle_state."

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(9)T and that functions in RPR+ mode. The symptom may also affect Release 12.4.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRI calls are being processed.

- CSCek55486

  Symptoms: The native Gigabit Ethernet (GE) interface on an NPE-G1 card may reset unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series when the underrun counter for the native GE interface increments continuously. You can verify the underrun counter in the output of the **show interfaces gigabitethernet** *slot/port* command.

  Workaround: There is no workaround.

- CSCek55511

  Symptoms: A Cisco AS5400HPX that is running Cisco IOS Release 12.3(11)T7 may crash with IO Memory corruption.

  Conditions: The crash may occur when polling for ccrpCPVGEntry, and resource pooling is enabled on the Gateway.

  Workaround: Disable SNMP polling for ccrpCPVGEntry.

- CSCek57655

  Symptoms: A modem autoconfiguration fails.

  Conditions: This symptom is observed in an asynchronous call.

  Workaround: There is no workaround.

- CSCsd50476

  Symptoms: A serial link goes down.

  Conditions: This symptom occurs when a T1/E1 controller that is configured with channel-group causes the serial link to go down. The CEM interface will not come up.

Workaround: There is no workaround.

- CSCse18355

  Symptoms: A Cisco AS5850-ERSC gateway reboots continuously with the message:

```
Bundled Rommon and FPGA versions are different from
the current system version. Updating the system.
This might take a while

System reload is required before upgrade can be done.
Rebooting the system ..
!
```

  Conditions: This symptom has been observed when a Cisco AS5850-ERSC gateway is running Cisco IOS interim Release 12.4(7.24)T.COMP.

  Workaround: Boot to ROM monitor mode and enter the following commands:

  SKIP_UPGRADE=1

  sync

  This step skips the upgrade process. To revert back, enter the following commands:

  unset SKIP_UPGRADE

  sync

- CSCse46964

  Symptoms: Periodic high CPU utilization on CMM modules which can cause performance issues such as poor voice quality, missed control and registration MGCP messages, slow response to command line interface. The **show process cpu history** command will display spikes of 100% utilization on the gateway even during hours where low activity is present. "%ALIGN-3-CORRECT: Alignment correction made at 0x601504F4 reading 0x2225F84A" error messages will be recorded when the CMM gateway is rebooted. This can be seen in the **show log** command if logging buffered is enabled on the gateway. When this problem occurs, the output of the **show alignment** command will display a high and increasing count value for the same address.

  Conditions: This symptom occurs when the CMM module is using Cisco IOS Release 12.4(8) or later releases, and the Catalyst 6000 supervisor module is a SUP720 that is running Native IOS.

  Workaround: There is no workaround.

- CSCse50887

  Symptoms: MGCP IOS Gateway sees the following:

```
%PARSER-4-BADCFG: Unexpected end of configuration file.
```

  and then:

```
config term router(UNKNOWN-MODE)
```

  Or, the **show running-config** command output is only 5 bytes.

  Conditions: This symptom occurs under the following conditions:

  - Use MGCP with the **ccm-manager config** command
  - Have more than 20 MGCP end points (voice ports)
  - Run Cisco IOS 12.3(11)T or later releases
  - Reset device pool from Cisco CallManager

Workaround: Add the **no ccm-manager config** command.

- CSCse69335

  Symptoms: Media Gateway Control Protocol (MGCP) FXS/FXO port and Cisco IOS T1CAS resets during Hookflash transfer with CCM being the call agent.

  Conditions: This condition is seen when two consecutive RQNT messages with S: rel event is received at the Cisco IOS gateway. In this condition, the second RQNT message will not be acknowledged by the Cisco IOS gateway. This results in reset of all the MGCP endpoints on the Cisco IOS gateway.

  Workaround: There is no workaround.

- CSCse89373

  Symptoms: A second PRI link gets deactivated, with no ability to process incoming and outgoing calls, when the second one is remotely, physically, manually (CLI command) deactivated.

  Conditions: This symptom occurs when the first PRI is type primary-net5, and the second PRI is type primary-qsig. Deactivate the second PRI remotely or locally by physically disconnecting the cable or issuing the **shutdown** command under the corresponding E1 controller.

  Workaround: There is no workaround.

- CSCsf03412

  Symptoms: The **boot flash** command or the boot TFTP crashes a router.

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Interim Release 12.4(7.24)T.

  Workaround 1: Use the **boot flash:** *image name* instead of **boot flash:** *imagename* command.

  Workaround 2: Use Cisco IOS Release 12.3(11)T.

  Workaround 3: Copy the image to flash and use the **boot flash:** *imagename* command, if the boot TFTP is the problem.

- CSCsf31178

  Symptoms: HWIC-1GE-SFP may experience an issue where the Gig Ethernet interface is “stuck” in a Line UP/Protocol Down state. While in this state, the interface will not pass traffic. Clearing the interface or manually disabling/enabling will clear the condition. This symptom does not occur when 1000BASE-T SFP is used.

  Conditions: A Loss of Signal (for example, unplugging the cable) may cause the interface to become stuck in a Line UP/Protocol Down state.

  Workaround: Clearing the interface or manually shutting it down, then bringing it back up will clear the problem.

- CSCsf95938

  Symptoms: There is a leak in middle buffers after all Onboard DSPRM Pools are depleted.

  Conditions: This symptom is observed on a Cisco 3800 series router that is running Cisco IOS Release 12.4(7b) with support for CVP survivability.

  Workaround: There is no workaround.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsg05350

  Symptoms: A Cisco AS5850 crashes due to a chunk memory leak. See the following:

  ```
  Sep  9 13:07:04.428: %DSMP-3-INTERNAL: Internal Error : NO MEMORY -Traceback=
  0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50 0x6127F6BC
  Sep  9 13:07:04.468: %DSMP-3-INTERNAL: Internal Error : NO MEMORY -Traceback=
  0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50 0x6127F6BC
  Sep  9 13:07:04.744: %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a
  reload due to Fragmented processor_memory, Free processor_memory = 10402472
  bytes, Largest processor_memory block = 522632 bytes
  ```

  Conditions: This symptom occurs when there is a chunk memory leak.

  Workaround: There is no workaround.

- CSCsg07907

  Symptoms: A Cisco 3845 router unexpectedly reloads with bus error as seen in the show version when enabling DSP mini logger (**voice dsp** *slot* command history enable).

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4 with conferencing enabled on the DSP slot that minilogger is being turned on for.

  Workaround: Disable conferencing on that slot, if possible.

- CSCsg08491

  Symptoms: A system may crash due to processor memory corruption.

  Conditions: This symptom may occur upon the application of a crypto map to an interface.

  Workaround: There is no known workaround.

- CSCsg09208

  Symptoms: A router that is running Cisco IOS may reload unexpectedly when applying an IPS policy to an interface.

  Conditions: This symptom is seen with version 6 SDF files on Cisco IOS Release 12.4(10) and later releases.

  Workaround: There is no workaround.

- CSCsg11718

  Symptoms: A VRF may become stuck in the “Delete Pending” state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- CSCsg12813

  Symptoms: A Cisco AS5400 gateway may change its RTP sequence numbers after receiving an MDCX command The RTP Stream SSRC is always the same, but the sequence number seems to be randomly initiated again.

Conditions: This symptom occurs when MGCP receives a modification request from PGW for echo cancellation three seconds after the call is established.

Workaround: There is no workaround.

- CSCsg15598

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.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.

- CSCsg18933

  Symptoms: A RIP route is learned from a RIP neighbor via a dialer interface (or other virtual interface type). When the neighbor disconnects and the interface goes down, the RIP route is removed from the RIP database. However, the RIP route remains in the routing table.

  Conditions:

  - RIP is configured with the **no validate-update-source** command.
  - RIP routes are learned via a virtual interface.
  - The virtual interface is using a negotiated address.
  - The problem is platform-independent.

  Workaround: Use the **clear ip route** command to remove the affected routes from the routing table.

- CSCsg28628

  Symptoms: NAS pkg asynchronous calls fail after a redundancy switchover has occurred, and the following error message is generated:

  Modems unavailable

  Conditions: This symptom is observed on a Cisco AS5850 that functions in RPR+ mode. This situation may impact service.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **redundancy switchover** command a couple of times to restore the Cisco AS5850 to normal operation.

- CSCsg58832

  Symptoms: Inconsistent lease times are seen on a router that is acting as DHCP relay agent. Lease expiration times may be reduced from the value specified by the server to as little as five minutes. The binding will then be deleted after the new lease time has expired.

  Conditions: This issue has been observed on a router that is running Cisco IOS Release 12.4T that is configured as DHCP relay agent. The **ip dhcp smart-relay** command must be configured for this issue to exist.

  Workaround 1: Remove the **ip dhcp smart-relay** command from configuration.

  Workaround 2: Renew the IP address on DHCP client.

- CSCsg69205

  Symptoms: On a Cisco PE router, “ip flow egress” configured on the PE-CE link does not capture traffic streams destined for the CE router.

  Conditions: This symptom occurs when the MPLS interface is a multilink interface.

  Workaround: Configure “mpls netflow egress” on the interface towards the CE. Afterwards, this command can be removed, and the traffic is still captured by netflow.

- CSCsg76715

  Symptoms: A device crashes while removing an ACE, which was *inserted* in the middle of the ACL rather than added at the end of the list.

  Conditions: This symptom occurs under the following conditions:

  1. If the *inserted* ACE has dest prefix length as 0 i.e.. *any* statement in place of dest addr, and
  2. ACL already has an ACE with same src prefix length and dest prefix length is greater than 0 (i.e.. other than any statement), and the *inserted* ACE should be lesser in seq no than this ACE, and
  3. The ACE with dest prefix length greater than 0 is deleted before deleting the inserted ACE.

  Workaround: Delete the Inserted ACE first (ACE with dest addr as any) and then delete the ACE with dest prefix length greater than 0 (or) deleting the complete ACL.

- CSCsg96462

  Symptoms: There is a memory leak in the SNASwitch process.

  Conditions: SNASwitch fails to free memory associated with maintaining the RTP history information when RTP pipes terminate under some conditions.

  Workaround: There is no workaround.

  Further Problem Description: The following messages may be seen when processor memory has been exhausted:

```
%SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x6016CEA0,
alignment 0
 Pool: Processor  Free: 1628716  Cause: Memory fragmentation
 Alternate Pool: None  Free: 0  Cause: No Alternate pool
 -Process= "SNA Switch", ipl= 0, pid= 64
```

  To check if memory is leaking do the following commands (note the exact upper/lower case used):

  show snasw rtp

  show memory summary | i GraphIt | Bytes

The first command will display all the RTP pipes. The second command will display a summary of all the memory with a "GraphIt" identifier. There should be approximately two blocks with the "GraphIt Client" identifier for each non-RSETUP RTP pipe.

If there are significantly more than two "GraphIt Client" blocks per RTP pipe, then SNASwitch is leaking memory.

Wide-Area Networking

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCek59078

  Symptoms: An L2TPv3 session is established when voluntary tunneling is configured and both peers have corresponding configurations. However, after configuring the pseudowire on UUT virtual-PPP interface, sessions on UUT and peer are UP, but "virtual-PPP1 is up, line protocol is down."

  Conditions: For this symptom to occur, the virtual-ppp interface was previously deleted using the **no interface virtual-ppp** *n* command, and then reinstated using the **interface virtual-ppp** *n* command.

  Workaround: Be certain that the virtual-PPP interface has never been unconfigured using the **no interface virtual- ppp** *n* configuration command since the router was booted.

- CSCek62099

  Symptoms: When PPP Multilink is enabled over a PPP over Ethernet (PPPoE) session, outbound packets are incorrectly sent without PPPoE headers. This causes them to be dropped.

  Conditions: This symptom is observed in Cisco IOS version 12.4 on all software- forwarding router platforms. It only affects packets which are not multilink encapsulated (due to the bundle only having a single link).

  Workaround: Either disable multilink PPP, or use the **ppp multilink fragment delay** interface command to force multilink headers to be applied to all outbound packets.

- CSCir00712

  Symptoms: When a LAC receives fragmented data traffic over an L2TP tunnel, the IP layer reassembles the packets and routes them over the wrong interface instead of processing them locally.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel. The symptom is release-independent.

  Workaround: There is no workaround.

- CSCsb24255

  Symptoms: A router may generate the following error message and a MALLOC failure may occur:

  ```
  flex_dsprm_voice_connect: voice tdm connect failed
  ```

  Conditions: This symptom is observed on a Cisco router that processes a large number of calls with a short call duration via an E1 PRI.

  Workaround: There is no workaround.

- CSCsf96318

  Symptom: QSIG (ISO) call back (ring back) fails between a Cisco 3745 router and a Cisco 1760 router.

  Conditions: The call back fails.

  Workaround: There is no workaround.

- CSCsg15642

  Symptoms: A PSTN Gateway unexpectedly restarts due to a lack of memory. Overtime memory utilization increases, and the **show processes memory sorted** command indicates that the ISDN process is allocating an increased amount of memory.

  Conditions: This leak occurs when a SETUP message with Display IE is received.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg40885

  Symptoms: A router crashes during Online Insertion and Removal (OIR) on MLP- PPP on a Cisco 7200 platform.

  Conditions: This symptom is observed on a Cisco 7200 router that is configured for MLP-PPP.

  Workaround: Shut the multilink interface before doing an OIR.

- CSCsg50202

  Symptoms:

  When BRI interface flaps rapidly, ISDN Layer 1 detects link down, but Layers 2 and 3 keep active state during the transition. This may cause the BRI interface to get stuck, where subsequent incoming/outgoing call is rejected.

  Conditions:

  The symptom may be observed when cable is pulled out and put back rapidly.

  Workaround:

  Issue the **clear interface** command or the **shutdown** command followed by the **no shutdown** command on the affected BRI interface.

- CSCsg56148

  Symptoms: Inbound GSM V.110 calls fail to train at a speed of 14400.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(10a)

Cisco IOS Release 12.4(10a) is a rebuild release for Cisco IOS Release 12.4(10). The caveats in this section are resolved in Cisco IOS Release 12.4(10a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCir00074

  Symptoms: A router crashes when the casnDisconnect object is set to “true” for a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series when you attempt to terminate the PPPoE session through SNMP by using the casnDisconnect object of the CISCO-AAA-SESSION-MIB.

  Workaround: There is no workaround.

- CSCsd26248

  Symptoms: A router set up to do dot1x authentication without accounting setup may experience a memory leak in process RADIUS until the process consumes all free memory.

  Conditions: This leak occurs on a router doing dot1x authentication without dot1x accounting configured and is sent attributes 24 (state) or 25 (class) from the Radius server.

  Workaround: There is no workaround.

- CSCsf19139

  Symptoms: %RADIUS-3-NOSERVERS messages are logged after a reload in Cisco IOS Release 12.3(18). At this time, the RADIUS accounting tickets are not generated.

  Conditions: This symptom has been observed on a Cisco AS5300 gateway.

  Workaround: Enter into configuration mode and change the order of the servers under the server group.

IP Routing Protocols

- CSCek14600

  Symptoms: A traceback has been seen on this release.

  Conditions: The symptom has been observed on Cisco IOS interim Release 12.4(04) T1fc2.

  Workaround: There is no workaround.

- CSCse29428

  Symptoms: A crash is seen with %ALIGN-1-FATAL after showing %SYS-2-CHUNKEXPANDFAIL and %SYS-2-MALLOCFAIL repeatedly.

  Conditions: This symptom is observed on a Cisco 3725 router that is running Cisco IOS Release 12.4(5a) with the c3725-advipservicesk9-mz image that is running IPSec VPN.

  Workaround: There is no workaround.

- CSCse56552

  Symptoms: Connections fail through a router that uses CBAC. The pre-gen session is created, and the download or transfer begins. The pre-gen session times out and gets deleted from the router. Since the full session never gets established, the connection then times out on the host.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(8) and using CBAC outbound on the outside interface when policy based routing is applied.

Workaround: There is no workaround.

Further Problem Description: This bug is first seen in Cisco IOS Interim Release 12.4(7.24).

- CSCse58419

  Symptoms: The memory consumption by the Chunk Manager process increases over time.

  Conditions: This behavior is observed on certain occasions when NAT is configured. When NVI with VRF is set in the system, the memory leaks rapidly. When NAT with VRF is set in the system, plus there is embedded address translation needed or skinny protocol traffic, the memory leaks in a slow pace.

  Workaround: There is no workaround.

- CSCse94682

  Symptoms: A Cisco router with EIGRP configured might generate an error message

  like:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6097922C  reading 0x70
  ```

  Conditions: The symptom only occurs if the **no ip next-hop-self eigrp** command is configured.

  Workaround: There is no workaround.

- CSCse98590

  Symptoms: The router will display SYS-2-MALLOCFAIL messages on the console, and various protocols will operate erratically as a result of a low memory condition.

  Conditions: When a router has to duplicate incoming IPv4 multicast packets for transmission on multiple interfaces, and one of those interfaces is a GRE tunnel operating in GRE IPv6 mode, then memory used to duplicate that packet stream will not be freed. As a result, the router will soon exhaust all available memory.

  Workaround: The router will not exhaust memory if packets do not need to be duplicated (for example, if they enter on one interface and only exit the box through another interface), or if they do not need to duplicate to a tunnel interface that is running GRE over IPv6 (for example, tunnel mode GRE IPv4 does not have this problem).

ISO CLNS

- CSCse85158

  Symptoms: Locally advertised networks that are configured for the NSAP address- family under BGP will not be readvertised once they have been cleared from the BGP table.

  Conditions: Once the **clear bgp nsap unicast *** command has been issued, the networks will no longer appear in the output of the **show bgp nsap unicast** command.

  Workaround: There is no workaround.

Miscellaneous

- CSCeg86867

  Symptoms: An AAA server does not authenticate.

Conditions: This symptom is observed on a Cisco platform that functions as an AAA server and that runs Cisco IOS Release 12.3(13) when you dial up using Microsoft callback through an asynchronous line. Dialup through an ISDN modem works fine.

Workaround: There is no workaround.

- CSCek50172

  Symptoms: An EEM policy with event interface can not be registered and traceback appears.

  Conditions: This symptom has been observed when configuring the EEM policy with event interface, and specifying a poll-interval larger than 2097151.

  Workaround: When configuring the EEM policy with event interface, specify poll- interval with value less than 2097151.

- CSCek52778

  Symptoms: Dialer idle timer is not reset by interesting traffic on ISDN NON- MLPP, Async MLPPP, Async PBR user sessions.

  Conditions: This symptom is found on a Cisco AS5850 that is running Cisco IOS Release 12.4(7b). Problem may occur with involvement of virtual profiles.

  Workaround: There is no workaround.

- CSCsb13010

  Symptoms: NAT configurations didn't go through due to insufficient memory.

  Conditions: This behavior was observed on a Cisco 831 router running Cisco IOS Interim Release 12.4(1.2)PI1a and also Interim Release 12.4(2.2)T.

  Workaround: There is no workaround.

- CSCse05642

  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

- CSCse64462

  Symptoms: A Cisco Systems 7200 series router may encounter a block overrun with Redzone corruption, and subsequently crash if Turbo ACL is configured and the following command is entered:

  ```
  clear eou all
  ```

Error messages similar to the following will be output, with associated tracebacks:

```
%SYS-3-OVERRUN: Block overrun at <address> (red zone <value>)
%SYS-6-BLKINFO: Corrupted redzone blk <address>
```

Conditions: This symptom is observed on a Cisco 7200 series router running Cisco IOS Release 12.4 that is configured for Turbo ACL and when the following command is entered:

```
clear eou all
```

Workaround: Disable Turbo ACL by entering the following command:

no access-list compiled

- 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

- CSCse75920

  Symptoms: A Cisco router experiences a memory leak for the processes SCCP application and Chunk manager.

  Conditions: The symptom has been observed after configuring the router for MTP and transcoding.

  Workaround: There is no workaround.

- CSCse89402

  Symptoms: The CPU stack frame may become corrupted when a channel-group is configured on the T1/E1 controller.

  Conditions: This symptom is seen on mainboard WIC slots when the slot is configured for the “no network-clock participate.”

  Workaround: Use the VWIC in “network-clock participate” when installed in the mainboard WIC slot of the router.

  Further Problem Description: In most situations, no problems are seen. In rare cases, a crash may occur.

- CSCse93695

  Symptoms: Three-way calls that involve the Broadsoft SIP server and Cisco IAD2400 series Integrated Access Devices may not work.

  Conditions: This problem is observed in Cisco IOS Release 12.4(9)T.

Workaround: There is no workaround.

- CSCse97112

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

  Conditions: This symptom is observed after the following command is issued:

  no x25 map compressedtcp a.d.c.d ip e.f.g.h [**options**]

  This may cause an Address Error (load or instruction fetch) exception, CPU signal 10.

  Workaround: There is no workaround.

- CSCsf03566

  Symptoms: Software-forced crash (SFC) occurs due to memory corruption.

  Conditions: The crash has been seen on a Cisco 7600 router running Cisco IOS Release 12.2(18)SXF5. This happens if the router is acting as an EZVPN sever and xauth is enabled when the crypto session is brought down.

  Workaround: There is no workaround.

- CSCsf09338

  Symptoms: The calls coming from the CMM MTP has one-way audio when a call transfer is done on the other side.

  Conditions: This symptom is observed when CMM is configured as MTP/XCode and running Cisco IOS Release 12.4(7b).

  Workaround: There is no workaround.

- CSCsf22493

  Symptoms: The Cisco Communication Media Module (CMM) crashes when processing the UnsubscribeDtmf message.

  Conditions: This symptom is observed when CMM XCODE/MTP is using Cisco IOS Release 12.4(8a) and RFC2833.

  Workaround: There is no workaround.

- 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

- CSCsg00602

  Symptoms: A Cisco 3845 or Cisco 3825 router with AIM-VPN/HPII-PLUS(EPII-PLUS) may show the following symptoms:

  1. Show alignment errors
  2. Crash by bus error
  3. XXX display by running the **show crypto engine accel ring packet** command
  4. If a Telnet session, which shows symptom 3, is cut by “clear line,” its related exec process does not disappear and starts to occupy CPU.

Conditions: This failure is seen on the Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 series routers that are configured with an AIM-VPNII or AIM-VPNII PLUS Virtual Private Network (VPN) encryption and hardware advanced integration module (AIM).

Workaround: Avoid running the **show crypto engine accel ring packet** command.

Wide-Area Networking

- CSCek55209

  Symptoms: If the **ppp multilink endpoint mac** *interface* command or the **ppp multilink endpoint ip** *a.b.c.d* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual-circuit is unconfigured.

  Conditions: This symptom is observed on a router with Multilink PPP.

  Workaround: Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCse12198

  Symptoms: Individual B-channels on the primary T1 in the NFAS group sometimes go OOS for no reason.

  Conditions: This symptom is observed when connected to a Cisco PGW that is running Cisco IOS Release 9.3(2). The Cisco AS5400 is connected to the Cisco PGW that is running RLM in the Signaling/Nailed mode.

  Also, sometimes ISDN service goes OOS, and also channel states goes to 5 which is maintenance pending.

  Workaround: When this happens, put ISDN service can be put back in service manually for individual CIC, but channel state cannot manually be put back in service unless the whole serial interface is bounced. This cannot be done when there is other traffic on the other b-channels.

- CSCse34162

  Symptoms: A Cisco router hangs after 5 to 10 minutes of passing traffic over a dialer interface.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 12.4(8) with PPP Multilink configured on a dialer interface and traffic is passing.

  Workaround: There is no workaround. A reboot is required to recover.

- CSCse81069

  Symptoms: Unconfiguring the **isdn service b_channel** command is not taking effect. The command is not removed from the running configuration.

  Conditions: This symptom occurs when configuring the **isdn service b_channel** command to a state other than the default value of 0 on the ISDN D channel.

  Workaround: To remove the command, shut down the T1/E1 controller first and then unconfigure the command under the D channel serial interface.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf03251

  Symptoms: Primary and backup NFAS interfaces may transition from WAIT to OOS even after receiving “in-service” message from the PSTN.

  Conditions: This symptom is observed on a Cisco AS5400XM that is running several Cisco IOS 12.4 mainline and 12.4T releases.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(10)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(10). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(10). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCek33076

  Symptoms: A RADIUS progress code is incorrectly reported for a call that fails at IPCP. The progress code reports that the Link Control Protocol (LCP) is the open state.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(3a) and that is configured for AAA.

  Workaround: There is no workaround.

- CSCek37174

  Symptoms: When you configure RADIUS servers via the AAA-SERVER-MIB, the expected behavior is that the last defined RADIUS server receives the lowest priority, but this does not occur.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA and that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCek40060

  Symptoms: RADIUS server authentication may not function for dialup and PPP clients.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) and that has the **radius-server retry method round-robin** command enabled.

  Workaround: Disable the **radius-server retry method round-robin** command. Note that the symptom does not occur in Release 12.3 or Release 12.3T.

- CSCin99788

  Symptoms: An %AAA-3-ACCT_LOW_MEM_TRASH error message is generated when a low-memory condition occurs. When this situation occurs, a memory leak may occur in AAA data.

  Conditions: This symptom is observed when an interface flaps and causes a very large number of sessions to go down simultaneously, in turn generating a very large number of accounting stop records. In this situation, the I/O memory may be held for a long time when accounting records are send and when an AAA server is slow or unreachable.

  Workaround: There is no workaround.

- CSCsc91735

  Symptoms: CyBus errors may occur during an HA switchover, causing most VIPs to be disabled on a Cisco 7500 series.

  Conditions: This symptom is observed when MLP Multilink interfaces are configured on channelized T3 (CT3) port adapters.

  Workaround: Reload microcode onto all affected VIPs.

- CSCsc97727

  Symptoms: An access point may crash when you add or remove TACACS servers via the CLI.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(7)JA1 or Release 12.3(7)JA2 and that has the **aaa accounting commands** *level* **default** *list-name* **group** *groupname* command enabled. The symptom may also occur in other releases.

  Workaround: Disable the **aaa accounting commands** *level* **default** *list-name* **group** *groupname* command.

  Alternate Workaround: Use RADIUS instead of TACACS.

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

  Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

  Workaround: There is no workaround.

- CSCsd49133

  Symptoms: Alarms are not populated in the ceAlarmTable and ceAlarmlist objects because the CISCO-ENTITY-ALARM-MIB does not function.

  Conditions: This symptom is observed on a Cisco router when a connected interface at a peer device is shut down. In this situation, alarms should be populated in the ceAlarmTable and ceAlarmlist objects. Note that the output of the **show facility-alarm status** EXEC command does show the alarms correctly, but they are just not populated in the ceAlarmTable and ceAlarmlist objects.

  Workaround: There is no workaround.

- CSCsd55847

  Symptoms: A ping does not go through completely.

  Conditions: This symptom is observed after you have entered the **microcode reload** command.

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

- CSCsd68168

  Symptoms: A VIP crashes with a bus error and illegal accesses to low memory addresses.

  Conditions: This symptom is observed when egress NetFlow is configured on a distributed platform such as a Cisco 7500 series router.

  Workaround: Enter the **ip flow egress** command on any interface after both the RP and VIP have come up or disable the **ip flow egress** command.

- CSCsd99763

  Symptoms: A Cisco 7200 series router reloads unexpectedly while configuring BGP access list.

Conditions: This symptom is observed on a Cisco 7206VXR (NPE-G1) processor (revision A). The following commands serve as an example that causes router to reload unexpectedly:

```
config t
   router bgp 100
   neighbor EXTERNAL route-map MAP3 out
   address-family ipv4 multicast
   neighbor EXTERNAL route-map MAP3 out
   !
   ip as-path access-list 1 deny ^$
   ip as-path access-list 2 permit ^(700)+(_1123)|_2374$|^(_700)+(_2374)+(_1123)+$
   ip as-path access-list 3 permit _3400_
   ip as-path access-list 4 permit ^(700)+(_3400)|_1123$|^700$|_23\[0-9\]$
   !
   route-map MAP3 permit 10
   match as-path 1
   !
   route-map MAP3 deny 20
   match as-path 2
   !
   route-map MAP3 permit 30
   match as-path 3
   !
   route-map MAP3 permit 40
   match as-path 4
   set metric 300
   end
```

Workaround: There is no workaround.

- CSCse08044

  Symptoms: A Cisco router may generate export packets in which the first flow record contains incorrect data such as incorrect IP addresses.

  Conditions: This symptom is observed on a Cisco router that is configured for NetFlow and NetFlow Data Export.

  Workaround: Disable NetFlow.

- CSCse09594

  Symptoms: A router crashes during the AAA authentication process for interfaces that are configured for PPP.

  Conditions: This symptom is observed on a Cisco router when the memory is exhausted. For example, the symptom may occur on a router that attempts to bring up more PPP sessions while its memory usage is already higher than 99 percent of the capacity because of existing configuration and sessions.

  Workaround: There is no workaround.

- CSCse13952

  Symptoms: After an SSO switchover has occurred on a PE router that functions in an AToM configuration, the standby RP may generate an "%ALIGN-1-FATAL: Corrupted program counter" error message, a bus error may occur, and the standby RP may crash.

  Conditions: These symptoms are observed when the **aaa accounting** command is enabled with a TACACs+ server in the following configuration:

  ```
  aaa accounting commands 15 default start-stop group tacacs+
  aaa accounting system default start-stop group tacacs+
  ```

  Workaround: There is no workaround.

- CSCse38956

  Symptoms: A router crashes when you change the authentication method after the user on the client side has entered the user name and is prompted to enter the password but has not yet entered the password.

  Conditions: This symptom is observed when you disable the **aaa authentication enable default group radius** command and enable the **aaa authentication enable default group tacacs** command, or the other way around, before the user on the client side has entered the password.

  Workaround: There is no workaround.

- CSCse49728

  Symptoms: SNMPv3 informs are not sent out after a device reload.

  Conditions: This symptom is observed when SNMPv3 informs have been configured, and the device is reloaded.

  Workaround: Re-enter any of the **snmp-server host** commands.

- CSCse52503

  Symptoms: An RSP may generate tracebacks.

  Conditions: This symptom is observed on a Cisco router that is configured for dCEF when you reload microcode onto the RSP. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse56743

  Symptoms: A standby RSP does not come but enters ROMmon mode.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 and that functions in an HA redundancy mode.

  Workaround: There is no workaround.

- CSCse69031

  Symptoms: The console of a Cisco 7500 series may hang when you perform an OIR of three or four VIPS.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.4(9.16).

  Workaround: There is no workaround.

- CSCse79528

  Symptoms: Serial and FDDI interfaces may not be detected.

  Conditions: This symptom is observed only on a Cisco 7500 series that has an RSP.

Workaround: There is no workaround.

- CSCse90357

  Symptoms: Onramp and offramp fax calls fail to connect over E1 PRI and E1 R2 signaling.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCse77357

  Symptoms: A router may reject the creation of virtual Token Ring interface with any interface number from 0 to 9 and allow only the creation of virtual Token Ring interface with an interface number that is equal to or greater than 10.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.16) or a later release or Release 12.4(9.15)T or a later release.

  Workaround: Manually configure the virtual Token Ring interface with a an interface number that is equal to or greater than 10.

IBM Connectivity

- CSCse17611

  Symptoms: When DLSw Ethernet Redundancy is configured, circuits may be established through the wrong switch.

  Conditions: This symptom is observed in the following configuration:

  - Clients are connecting to MAC A.
  - Mapping statements are configured so that Switch 1 has a mapping of MAC A = MAC A and Switch 2 has a mapping of MAC B = MAC A.

  The output of the **show dlsw transparent map** shows that Switch 1 has the active mapping and that Switch 2 has the passive mapping. All circuits should be established on Switch 1, but instead they are established on switch 2.

  The outputs of the **show dlsw trans neighbor** and **show dlsw trans map** commands show correct information, but the output of the **show dlsw cir cache** command shows state “negative” on Switch 1 and state “positive” on Switch 2.

  Workaround: There is no workaround. Note that all circuits are up and running, but they just go through the wrong router.

Interfaces and Bridging

- CSCek27833

  Symptoms: Pings with a datagram size of 1485 and above are not going across the bridge.

  Conditions: This symptom is observed on a serial interface configured for PPP and part of the bridge group on a Cisco router.

Workaround: Increase the MTU size on the interfaces. For example, configure an MTU of 1524.

- CSCin97786

  Symptoms: An online insertion and removal (OIR) of a Versatile Interface Processor (VIP) that is installed in a Cisco 7500 series may cause the Route Switch Processor (RSP) to stop responding.

  Conditions: This symptom is observed when two FDDI port adapters are installed in the VIP.

  Workaround: There is no workaround.

- CSCsc66187

  Symptoms: Error messages such as the following one may be generated on a Cisco 7500 series or Cisco 7600 series:

  ```
  %CWPA-3-IPCALLOCFAIL: Failed to allocate IPC buffer for loveletter data
  ```

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured with a 1-port Packet-over-SONNET OC-3c/STM-1 multimode port adapter (PA-POS-OC3MM) when you enter the **no shutdown** interface configuration command on the interface.

  Workaround: There is no workaround.

- CSCse17103

  Symptoms: A Bridge Group Virtual Interface (BVI) stops receiving CLNS packets.

  Conditions: This symptom is observed when the packets arrive via a dot1q subinterface that belongs to one bridge group and when another dot1q subinterface on the same physical interface belongs to another bridge group.

  Workaround: Enter the **clns router isis** *area-tag* command on the physical subinterface.

  Alternate Workaround: Enter the **clns enable** command on the dot1q subinterface, although doing so may cause problems with the connected end systems.

- CSCse61893

  Symptoms: A ping from a channelized T3 (CT3) port adapter may fail.

  Conditions: This symptom is observed on a Cisco platform that is configured with a CT3 port adapter that functions in unchannelized mode.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed84633

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

  Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206. 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 fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCej78303

  Symptoms: A router may crash when you disable the **ipv6 multicast-routing** command.

  Conditions: This symptom is observed when you enable and disable the **ipv6 multicast-routing** command multiple times while IPv6 Multicast traffic is being processed.

  Workaround: There is no workaround.

- CSCek29860

  Symptoms: A Cisco router may experience a software-forced crash.

  Conditions: This symptom is observed on a Cisco router that is configured for secure NAT (SNAT), NAT Stateful Failover, and HSRP.

  Workaround: There is no workaround.

- CSCek31478

  Symptoms: When you modify an access control list (ACL) by entering the **ip multicast boundary** command, the command may not fully take effect.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 or Release 12.0(32)S but appears to be platform- and release-independent.

  Workaround: Disable and re-enter the **ip multicast boundary** command.

  Alternate Workaround: Enter the **clear ip mroute *** command.

- CSCek42134

  Symptoms: NAT Virtual Interface (NVI) per VPN routing/forwarding (VRF) is broken from inside to outside. The router shows CEF drops for the destination prefix existing for a route for this prefix on VRF table.

  Conditions: This symptom has been observed on Cisco IOS Release 12.3(14)T6 and interim Release 12.4(7.20)T.

  Workaround: Configure static translation for the destination prefix to itself.

- CSCek43945

  Symptoms: A memory leak may occur on a router that is configured for NAT and the router may eventually run out of memory.

  Conditions: This symptom is observed on a Cisco router when NAT is configured.

  Workaround: There is no workaround.

- CSCsc35609

  Symptoms: In certain circumstances, if the static reservations are configured via the **ip rsvp listener** commands, an interface going down can cause the router to crash.

  Conditions: This problem is seen under the following conditions:

  1. Router is running RSVP; the **ip rsvp bandwidth** command is enabled.
  2. Router has configured a receiver proxy with the **ip rsvp listener** command.
  3. Router receives Path messages matching the proxy and sends out Resv messages corresponding to the received Path messages.
  4. The interface on which the Path message is received goes down.

  The problem is not seen if any of these conditions do not hold. For example, routers not running RSVP, or running RSVP only as a midpoint, or routers running MPLS/TE, do not see this problem.

Workaround: There is no workaround. Discontinuing the use of the **ip rsvp listener** command will prevent the crash.

- CSCsc75426

  Symptoms: A router that is configured for BGP and that has the **ip policy-list** command enabled may unexpectedly reload because of a bus error or SegV exception.

  Conditions: This symptom is observed when BGP attempts to send an update with a “bad” attribute.

  Workaround: There is no workaround.

- CSCsd03021

  Symptoms: When loading a large link state database from a third-party vendor router that runs Cisco IOS software, the CPU usage by OSPF may become very high, the router may generate CPUHOG messages, and it may take a long time to reach the FULL state, or the FULL state is not reached.

  Conditions: These symptoms are observed in an environment in which packet drops occur. When the link state request that is sent from the Cisco IOS router is dropped, the routers may still continue to exchange DBD packets. However, the link stay request list on the Cisco IOS router may become long, and it may take a lot of CPU usage to maintain it.

  Workaround: There is no workaround.

  Further Problem Description: See also caveat CSCsd38572.

- CSCsd68993

  Symptoms: IPv6 multicast traffic forwarding may fluctuate.

  Conditions: This symptom is observed on a Cisco router that is configured for PIM and that is configured with more than 2000 multicast streams.

  Workaround: There is no workaround.

- CSCsd84489

  Symptoms: A platform that is configured for Open Shortest Path First (OSPF) and incremental Shortest Path First (SPF) may crash when changes occur in the OSPF topology.

  Conditions: This symptom is observed on a Cisco platform that has the **ispf** command enabled when changes occur in the OSPF topology that cause the intra-area routes to be updated.

  Workaround: Disable the **ispf** command.

- CSCse04037

  Symptoms: A ping or a Telnet connection from an inside gateway to an outside gateway through a router that is configured for NAT may fail because of an error in the NAT table lookup process.

  Conditions: This symptom is observed on a Cisco router when the **preserve-port** keyword is not configured in the **ip nat service** command and occurs whether or not NAT Overload is configured.

  Workaround: There is no workaround.

- CSCse04220

  Symptoms: The BGP table version remains stuck at 1, and the router may crash.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for an ATM network service access point (NSAP) address family.

  Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

- CSCse07118

  Symptoms: A router may reload unexpectedly when using the **transmit- interface** interface command when there is an OSPF point-to-point adjacency in the interface.

  Conditions: The unexpected reload is seen when the OSPF is point-to-point, either because it is, for example, a serial interface, or when using the **ip ospf network point-to-point** interface-level configuration command.

  Workaround: Issue a **shutdown** command before using the **transmit-interface** command if there is an OSPF adjacency in the interface being configured.

- CSCse44079

  Symptoms: The CPU usage may reach 100 percent in the IGMP Input process when a ULD interface is down.

  Conditions: This symptom is observed on a Cisco router that has a UDL interface that is connected to a satellite link after you have upgraded the Cisco IOS software image from Release 12.4(5a) to Release 12.4(7a).

  Workaround: There is no workaround.

- CSCse51804

  This caveats consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

     Condition 1: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4 when the DMVPN tunnel is up and when you enter the **show ip nhrp brief** and **clear ip nhrp** commands. When the tunnel comes up again (because of the NHRP registration by the spoke), the NHRP cache entry expires a long time before its expiration time.

     Workaround 1: Do not enter the **show ip nhrp brief** command.

  2. Symptom 2: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

     Condition 2: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4(6)T or a later release and occurs without any specific action.

     Workaround 2: There is no workaround.

- CSCse55265

  Symptoms: A ping fails via NAT because of an encapsulation failure.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for NAT and that has both the **ip nat inside source static** and **ip nat outside source static** commands enabled. The symptom is platform-independent.

  Workaround: There is no workaround.

ISO CLNS

- CSCsd87651

  Symptoms: A Cisco router that is configured for RPR or RPR+ may reload its standby RP when a configuration change is made to IS-IS.

  The reload of the standby RP is proceeded by the following error messages:

```
%HA-3-SYNC_ERROR: Parser no match. %HA-5-SYNC_RETRY: Reloading standby and retrying
sync operation (retry 1).
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4. Note, however, that the symptom is platform-independent for Release 12.4 and its derivatives. Any of the IS-IS global configuration commands may trigger the symptom. Following are a few examples of these IS-IS global configuration commands:

- `is-type level-2-only`
- `lsp-gen-interval level-2 5 50 100`
- `redistribute eigrp`

Workaround: There is no workaround.

- CSCse40346

  Symptoms: Tracebacks may be generated when you configure IS-IS and LDP features, for example, when you enter the **no ip router isis** *area-tag* command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)SY but may also occur in other releases.

  Workaround: There is no workaround.

- CSCuk60585

  Symptoms: A router that is configured for redistribution into ISO-IGRP may crash.

  Conditions: This symptom is observed when the configuration is nvgened.

  Workaround: There is no workaround.

Miscellaneous

- CSCef09119

  Symptoms: CPUHOG tracebacks may be generated when you bring up 30,000 PPPoE sessions and then remove an input policy map from a virtual template on a broadband PTA.

  Conditions: This symptom is observed on a Cisco router that functions as a broadband PTA and that is configured with 31,500 ATM subinterfaces, an input policy map, an output policy map with an CBWFQ policy, and 128,000 queues.

  Workaround: There is no workaround.

- CSCef29090

  Symptoms: The throughput for TCPClear sessions on a Cisco AS5850 may not be as expected and there may be a slow response time.

  Conditions: This symptom is observed on a Cisco AS5850 with TCPclear sessions.

  Workaround: There is no workaround.

- CSCeh86525

  Symptoms: A router crashes when you attach an inbound service policy with a police feature.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 that supports Multiprocessor Forwarding (MPF).

  Workaround: There is no workaround.

- CSCei84353

  Symptoms: A router crashes when you remove an Embedded Event Manager (EEM) applet.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S but is not platform- and release-dependent. This symptom occurs under the rare occasion that the EEM applet is removed while EEM is attempting to trigger the applet for execution.

Workaround: Perform the following three steps:

1. Before you remove the EEM applet, disable EEM applet scheduling by entering the **event manager scheduler applet suspend** command.
2. Remove the applet.
3. After you have removed the applet, re-enable EEM applet scheduling by entering the **no event manager scheduler applet suspend** command.

- CSCej29710

  Symptoms: Unable to send EEM type system SNMP trap notifications.

  Conditions: This symptom occurs when users want to send EEM SNMP system type trap notifications upon triggering of a policy.

  Workaround: In EEM applet mode if a user desires an SNMP notification upon event trigger, they should specify it as an action by using the **action snmp-trap** command. In EEM TCL policies, use the **action_snmp_trap** TCL command.

- CSCek26155

  Symptoms: A recursive pattern scan loop can occur when the Embedded Event Manager (EEM) CLI ED attempts to scan for patterns provided by action CLI commands.

  Conditions: This issue occurs when an applet contains a CLI event that is scanning for a pattern that is given as a CLI command in one of its actions. See the following example:

```
event manager applet one
   event cli pattern "show version" sync yes
   action 1 cli command "show version"
```

  In this example the action being performed causes the event to trigger in a loop.

  Workaround: Do not use an action CLI command containing a pattern that matches the CLI event pattern.

- 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

- CSCek34049

  Symptoms: A Cisco AS5850 that is configured for RPR+ may be unable to process more than 1990 MGCP voice calls. With more than 1990 MGCP voice calls, any of the following symptoms may occur:

  – Many DSP may time-out.

  - Active calls may hang.
  - Spurious memory accesses and tracebacks may be generated.
  - Incoming calls may be dropped.
  - NextPort SPE ports may be stuck in the “a” state.

  Conditions: These symptoms are observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(3d) or Release 12.4(7a).

  Workaround: There is no workaround. A Cisco AS5850 that is used to its full capacity (4 CT3 worth of MGCP calls) may not scale beyond 1990 calls. When the symptoms have occurred, reload the Cisco AS5850.

- CSCek37686

  Symptoms: A Cisco AS5350 may reload because of a bus error (SIG=10).

  Conditions: This symptom is observed when SNMP is configured and when SNMP queries are made into the Cisco AS5350.

  Workaround: Disable SNMP or stop polling the router.

- CSCek38136

  Symptoms: When you deploy VoIP using PVDM2 / 5510 DSP modules, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with 5510 DSP modules. The symptom does not occur with 549 DSP modules.

  Workaround: There is no workaround.

- CSCek41338

  Symptoms: A router reloads when you enter the **peer default ipv6 address pool** *pool-name* command in template-configuration mode.

  Condition: This symptom is observed on a Cisco router that is configured for IPv6.

  Workaround: A workaround is not applicable because the **peer default ipv6 address pool** *pool-name* command in template-configuration mode is not supported in an IPv6 configuration and should not be entered as such.

- CSCek42816

  Symptoms: A voice gateway reloads while bulk calls are being processed.

  Conditions: The symptom is observed on a Cisco voice gateway that runs VXML applications that stream voice when the voice gateway receives prompts from an HTTP server.

  Workaround: Enter the **ivr prompt streamed none** command on the voice gateway.

- CSCek43562

  Symptoms: After an SDM client has properly connected to an SSH server, the SDM client hangs when you attempt to close the connection.

  Conditions: This symptom is observed only with an SDM client, which uses a third-party vendor Java-based SSH client package.

  Workaround: There is no workaround.

- CSCek43642

  Symptoms: When you try to remove an Embedded Event Manager (EEM) policy that has event criteria specified via the **event_register_appl** Tcl command extension, the attempt fails.

Conditions: This symptom is observed when two or more Embedded Event Manager policies are configured and when only one of these policies has event criteria specified via the **event_register_appl** Tcl command extension.

Workaround: There is no workaround.

- CSCek45461

  Symptoms: Path confirmation fails for voice calls on a Cisco AS5850. One-way audio may occur with manual phones.

  Conditions: These symptoms are observed on a Cisco AS5850 that processes MGCP, H.323, and SIP calls.

  Workaround: There is no workaround.

- CSCek47283

  Symptoms: A router cannot be reloaded by entering the **reload** command, and the following message is displayed when you attempt to reload the router:

  ```
  The startup configuration is currently being updated. Try again.
  ```

  Conditions: This symptom is observed under rare conditions and may be triggered after an "Invalid pointer value in private configuration structure" error message is displayed (as seen in caveat CSCin98933). This symptom is observed in Cisco IOS interim Release 12.3(19.7), interim Release 12.4(6.5), and interim Release 12.4(6.5)T, and in later releases.

  Workaround: There is no workaround.

- CSCek47653

  Symptoms: A voice gateway may crash because of a bus error that is related to an MGCP Visual Message Waiting Indicator (VMWI) function.

  Conditions: This symptom is observed on a Cisco IAD 2430 that runs Cisco IOS Release 12.3(14)T2. The symptom may also affect Release 12.4 and Release 12.4T.

  Workaround: There is no workaround.

- CSCin97669

  Symptoms: The standby RP resets continuously because of synchronization failures.

  Conditions: This symptom is observed on a Cisco router when you first perform and OIR of a VIP in which a port adapter is installed that supports both T1 and E1 (for example, a PA-MC-8TE1+ port adapter) and then an SSO switchover occurs.

  Workaround: There is no workaround. You must power-cycle the standby RP to enable it to come up.

- CSCin99565

  Symptoms: A router that is configured for SSG may reload unexpectedly.

  Conditions: This symptom is observed when both the Transparent Auto-Logon (TAL) and Port-Bundle Host-Key (PBHK) SSG features are enabled and when it takes a long time before the AAA server responds.

  Workaround: There is no workaround.

- CSCin99687

  Symptoms: An SNMP walk of the dsx1IntervalTable results in an infinite loop.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MCX-8TE1 or PA-MC-2T3+ port adapter.

  Workaround: There is no workaround.

- CSCsa70712

  Symptoms: When you reload a CMM in one slot, the CMM in another slot reloads too, and the console of the supervisor engine shows an "EarlRecoveryPatch Reset" error message for the CMM that you intentionally reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series when you enter the **reload** command via the console of the CMM.

  Workaround: Do not reload the CMM via its console. Rather, enter the **hw-module module** *slot number* **reset** command for the CMM on the supervisor engine.

- CSCsb42470

  Symptoms: The output of the **show interfaces sum** and the **show interfaces tunnel** commands is inconsistent.

  Conditions: This symptom is observed when CEF switching is enabled and when IPsec tunnel protection or VTI is applied to a tunnel interface.

  Workaround: Disable CEF switching and use fast-switching or process-switching.

  Further Problem Description: The output of the **show interfaces tunnel** command shows the wrong number of packets that are switched per second, and the number of bytes that have been switched is shown incorrectly.

- CSCsb54378

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

  Conditions: This problem has been observed when initiating a Secure Shell (SSH) session from the router or when copying a file to/from the router via SCP.

  Workaround: Do not initiate SSH or SCP sessions from the router.

  Further Problem Description: This was observed on a Cisco 2811 router that was running Cisco IOS Release 12.4(4)T.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash with %SYS-2-WATCHDOG. See the following example:

  ```
  *Mar 29 11:29:35.938: %SYS-3-CPUHOG: Task is running for (128004)msecs, more than
  (2000)msecs

  (1426/5),process = Virtual Exec.

  -Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768
  0x41BA7490 0x41BA7750

  0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8
  0x41834200

  *Mar 29 11:29:35.942: %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process
  = Virtual Exec.

  -Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490
  0x41BA7750 0x41BAC854

  0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200
  0x418341E4

  %Software-forced reload
  ```

- CSCsb95563

  Symptoms: On rare occasions, Embedded Event Manager (EEM) may cause a crash when you deregister an EEM policy.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series but is platform-independent.

  Workaround: There is no workaround.

- CSCsb99936

  Symptoms: The **show ephone** command reveals a call is stuck in the SEIZE state instead of progressing to the correct state during a call.

  Conditions: This symptom has been observed when an H.323 call is placed from CME to a non-CME H.323 endpoint.

  Workaround: There is no workaround.

- CSCsc12255

  Symptoms: When you deploy VoIP on an NM-HDV2 network module that is configured with a PVDM2-64 module, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with an NM-HDV2 network module. Note that the symptom does not occur with an NM-HDV network module.

  Workaround: There is no workaround.

- CSCsc13670

  Symptoms: The backup configurations that are generated by the Archive feature may be truncated.

  Conditions: This symptom is observed when you reload the router with the Archive feature enabled.

  Workaround: Enter the privileged mode.

- CSCsc18707

  Symptoms: No error message is printed out when running an Embedded Event Manager (EEM) policy that is not registered with the none event detector.

  Conditions: This symptom occurs when executing **event manager run** *policy name* or **action label policy** *policy name* command, but the policy is not registered with the none event detector.

  Workaround: There is no workaround.

- CSCsc41527

  Symptoms: The **chkflash** command for a flash file system does not function.

  Conditions: This symptom is observed on a Cisco router that has a flash file system.

  Workaround: Do not enter the **chkflash** command. Rather, enter the **format** command.

  Further Problem Description: The fix for this caveat re-implements the **fsck** command.

- CSCsc70644

  Symptoms: A CLI session may become stuck during the configuration of QoS.

  Conditions: This symptom is observed on a Cisco router after you have entered the **show policy-map interface** command.

  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.

- CSCsc72828

  Symptoms: Sweep ping with packet size 1439 fails.

  Conditions: This symptom occurs when dLFIoATM is configured on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCsc97398

  Symptoms: The user information Layer 1 protocol may be included in the outgoing bearer capability and may be set to either G711 u-law or G711 A-law. Some PBXs may refuse the call because of this mismatch in the bearer capability.

  Conditions: This symptom is observed when a call is made from H.323 to ISDN with unrestricted digital information bearer capability.

  Workaround: There is no workaround.

- CSCsd04075

  Symptoms: The voice ports of a Cisco IOS Voice over IP (VoIP) gateway that terminates fax calls may lock up and not accept any new calls. The following error messages may be generated on the console or syslog (if enabled):

  ```
  %HPI-3-CODEC_NOT_LOADED: channel:2/0/0 (171) DSP ID:0x1, command failed as codec not loaded 0

  - Traceback= 615D2FA8 615C8528 617D5044 617D5258 61BBCD44 61BBD764 617BAE88 617BBD38 6138720C
  ```

  Conditions: This symptom is observed on a Cisco 3600 series router but is not platform-dependent.

  Workaround: Disable T.38 and use fax passthrough.

- CSCsd07028

  Symptoms: Tracebacks may be seen when issuing the **clear pppoe all** command while unconfiguring the virtual circuit (VC).

  Conditions: This symptom is observed when a Cisco router crashes when the PPPOE session is cleared by issuing the **clear pppoe all** command.

  Workaround: There is no workaround.

- CSCsd16006

  Symptoms: Stale routing entries may be created on a Cisco MWG Home Agent (HA) when a mobile node (MN) deregisters or is handed off (that is, the MN moves from one foreign agent to another foreign agent). This situation affects the routing of mobile traffic.

  Conditions: This symptom is observed when NAT Traversal (NAT-T) is enabled and applied to mobile bindings.

  Workaround: There is no workaround.

- CSCsd18739

  Symptoms: When a router is configured for IPv6-NAT-PT the router goes into a software forced reload when the **show ipv6 nat translations verbose** command is executed. The following error message is displayed:

  ```
  %Software-forced reload Preparing to dump core...
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(3b).

  Workaround: Do not execute the **show ipv6 nat translations verbose** command.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that runs Cisco IOS Release 12.4(3b)B. The router has services 81, 82 and 90 configured. The only service that has a problem is 90. The packet traces indicate that the router is sometimes responding to “Here_I_Am” messages from the cache with “I_See_You” messages that contain an incorrect destination IP address. This situation leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3b) but may also affect other releases.

  Workaround: There is no workaround.

- CSCsd34114

  Symptoms: A router that has the **ip local pool** command enabled in an IPv6 configuration may reload under rare circumstances.

  Conditions: This symptom is observed when the local pool must allocate prefixes to the same user name on multiple interfaces in a specific order, then releases one of the prefixes, and then attempts to allocate a new prefix.

  The interfaces that the prefixes are allocated on, and the ordering of the events, must follow a very specific pattern in order for the symptom to occur.

  Workaround: Use per-user prefixes from a RADIUS server, or in a DHCP-PD configuration, use the prefix allocation per DUID.

  Further Information: IP local pools in an IPv6 configuration are used by DHCP-PD and by IPv6 Control Protocol (IPv6CP) for IPv6 over PPP links. However, the symptom is unlikely to occur with IPv6CP.

- CSCsd34529

  Symptoms: A Cisco router may crash when a policy map is simultaneously displayed and unconfigured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T but may also affect Release 12.4. The symptom occurs when the **show policy-map** command is entered via one CLI session while the **no policy-map** *policy-map-name* command is entered via another CLI session.

  Workaround: There is no workaround.

- CSCsd35555

  Symptoms: The TDM crossconnect for a T1/E1 WIC does not function.

  Conditions: This symptom is observed on a Cisco IAD 2400 series that is configured with a VIC2-2MFT-T1/E1 WIC.

  Workaround: Use the native T1/E1 slot to install the WIC in.

- CSCsd37629

  Symptoms: Alignment errors and a bus error may occur on a Cisco platform that has the **ip inspect** command enabled.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: Disable the **ip inspect** command.

- CSCsd41586

  Symptoms: When issuing a **show running-config** command, a system might experience a crash due to bus error.

  Conditions: This symptom was seen when the **show startup-config** command was still in progress in another terminal window and output did not finish yet.

  Workaround: Make sure that **show startup-config** command is not in use when issuing a **show running-config** command.

  Further Problem Description: This issue has only been seen on a Cisco 10000 series router but could affect other systems as well. Other concurrent access to NVRAM could lead to similar problems.

- CSCsd57360

  Symptoms: A software crash may occur on a Cisco 3700 series that is configured with a VWIC2-2MFT-T1/E1 when you first enter the **clock source independent** command on the T1 controller and then configure a channel group.

  Conditions: This symptom is observed when the following sequence of events occurs:

  1. You remove the channel group configuration from the T1 controller.
  2. You enter the **clock source independent** command on the T1 controller and you either set the clock source to internal or to line.
  3. You configure a channel group.

  Workaround: Do not enter the **clock source independent** command.

- CSCsd62621

  Symptoms: Packet loss in the form of ignores and overruns may occur on a Cisco 2621XM with a WIC-2T when you enter any of the following commands:

  - `write memory`
  - `show running-config`
  - `show controllers`

  Conditions: This symptom is observed on a Cisco 2621XM that runs Cisco IOS Release 12.4(7) when the serial port of the WIC-2T clocks at 8 Mbps and when 6.61 Mbps of traffic runs bidirectionally through the interface.

  Workaround: Do not enter the **write memory**, **show running-config**, or **show controllers** command while the serial port of the WIC-2T is processing traffic.

- CSCsd65073

  Symptoms: A PE router crashes while reconfiguring Multicast Virtual Routing and Forwarding (MVRF) with different default MDT address after removing the previous default MDT address.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(7.15). The PE router is configured with two MVRFs.

  Workaround: There is no workaround.

- CSCsd65289

  Symptoms: When applying a service-policy to a subinterface, the router crashes.

  Conditions: This problem happens on an ATM subinterface with a large amount of subinterfaces with service-policies applied.

  Workaround: There is no workaround.

- CSCsd66800

  Symptoms: A gateway-controlled T.38 fax relay between an MGCP gateway and another gateway may be disconnected unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that is configured for Voice xGCP.

  Workaround: There is no workaround.

- CSCsd70119

  Symptoms: A Media Termination Point (MTP) does not generate an RFC 2833 event on a second call leg when it should do so.

  Conditions: This symptom is observed when a call from a CallManager version 5.0 invokes an MTP and an RFC 2833 event and when the call is supported on both endpoints that are connected via the MTP.

  For example, a Cisco 7860 IP phone that is configured for SCCP sends a DTMF via both SCCP and RFC 2833. In this situation, the MTP receives an RFC 2833 event from the Cisco 7860 IP phone and a SCCP DTMF notification from the CallManager for the same DTMF event. This function properly, but the MTP does not generate the RFC 2833 event on the second call leg when it should do so.

  Workaround: In the above-mentioned example, disable RFC 2833 DTMF on the Cisco 7860 IP phone.

- CSCsd73526

  Symptoms: When a Cisco Content Services Switch (CSS) is used in a Customer Voice Portal (CVP) configuration, the Cisco IOS Voice Browser may be unable to play the media file. The CSS does send the HTTP Redirect message that points to the CVP, but the gateway does not react.

  Conditions: This symptom is observed on a Cisco AS5400HPX Universal Gateway after you have upgraded this platform from Cisco IOS Release 12.3(3a) to Release 12.4(3b). Other software components in the configuration are CVP 3.1 SR1, ICM 6.0, and Cisco CallManager 4.1(3)SR2.

  Workaround: Bypass the Cisco CSS, and point the VXML application directly to the CVP.

- CSCsd74000

  Symptoms: A slot controller such as a slot controller of a VIP4-80 may reset because of a TLB (load or instruction fetch) exception.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(17b) or Release 12.4, that has T1 or E1 port adapters installed in the slot that is controlled by the slot controller that resets, and that has NBAR configured.

  Workaround: Remove the NBAR configuration.

- CSCsd74729

  Symptoms: A crypto map may become “incomplete” and IPsec negotiation may fail.

  Conditions: This symptom is observed on a Cisco platform when the **ip vrf forwarding** *vrf-name* interface configuration command is removed from an interface or changed.

  Workaround: Remove and re-apply the crypto map configuration to the interface.

- CSCsd76444

  Symptoms: A Cisco router may reload unexpectedly with a “Signal 0” without a stack trace in the crash info file.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE and that is configured for SSG. However, the symptom is platform-independent and may occur on any router that is configured for SSG.

Workaround: There is no workaround.

- CSCsd76528

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: None of the policy classes after the first child policy of a hierarchical QoS policy take effect when you reload the router.

     Condition 1: This symptom is observed on a Cisco 7304 that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **service-policy output** interface configuration command to enable the child policies to take effect. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

  2. Symptom 2: On a Cisco 10000 series that is configured with hierarchical queueing policies, when you remove the **match vlan** command for a VLAN that matches a dot1q subinterface, the queues that are allocated to the subinterface are not cleared, allowing traffic to continue to flow through these queues.

     Condition 2: This symptom is observed on a Cisco 10000 series that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

     Workaround 2: There is no workaround. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

- CSCsd79195

  Symptoms: An I/O memory leak may occur on a Cisco router that is configured with an 8-port async/sync serial network module (NM-8A/S) and hardware crypto accelerators.

  Conditions: This symptom is observed when the **qos pre-classify** command is enabled on the crypto map and tunnel interface.

  Workaround: Disable the **qos pre-classify** command.

- CSCsd80745

  Symptoms: A router that is configured for IPSec and ISAKMP may reload unexpectedly because of a bus error exception that is triggered by an address error exception.

  Conditions: This symptom is observed rarely and occurs when data leaks during IPSec rekeying. Both IPSec and ISAKMP life times are configured as the recommended values of respectively 3600 seconds and 86,400 seconds. The router may crash when the data is used 65,536 times.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  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.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

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

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCsd85852

  Symptoms: When a PVC is shut down on the remote side, the PVC subinterface on a router transitions from the down state to the up state within one second, but then remains in the down state after the down retry timers expire.

  Conditions: This symptom is observed on a Cisco router that is configured for Operation, Administration, and Maintenance (OAM) and Dynamic Bandwidth Selection (DBS).

  Workaround: There is no workaround.

- CSCsd87399

  Symptoms: When the globally unique identifier (GUID) header is configured in the base-16 format, about 40 percent of the SIP calls may fail with a “500 response”.

Conditions: This symptom is observed in a normal configuration on a gateway and dial peers when the GUID header is configured in the base-16 format (that is, with 35 characters) instead of the base-10 format (that is, with 43 characters).

Workaround: There is no workaround.

- CSCsd87652

  Symptoms: On a Cisco 7200 series router, random packet drops are seen when a GRE tunnel fragments packets, and the tunnelled packets are encrypted.

  Conditions: The problem is seen on a Cisco 7200 series router when CEF is configured, and fragmentation occurs on the tunnel, and a crypto map is configured on the physical output interface.

  Workaround: Disable CEF.

- 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.

- CSCsd93522

  Symptoms: An NPE-G2 crashes when you first enter the **no ima-group** command, then you enter the **atm vc** command for the IMA group, and finally you enter the **show vc** command.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an IMA port adapter.

  Workaround: First configure an IMA group. Then, configure a VC for this IMA group.

- CSCsd93833

  Symptoms: A router may reload when you unconfigure an ATM TDM connection on an E1 controller.

Conditions: This symptom is observed on a Cisco 3600 series router.

Workaround: There is no workaround.

- CSCsd98525

  Symptoms: An SSH version 2 (SSHv2) session is terminated prematurely.

  Conditions: This symptom is observed when large chunks of data are transferred in the SSHv2 session, for example, when the **show tech** command is entered and the command output is transferred in the SSHv2 session.

  Workaround: Use SSH version 1.

- CSCse01124

  Symptoms: The Hot Standby Router Protocol (HSRP) may not come up and may remain in the "Init" state, which can be verified in the output of the **show standby brief** command.

  Conditions: This symptom is observed when dampening is configured on a native Gigabit Ethernet interface of a Cisco 7200 series or on a Fast Ethernet interface of a PA-FE-TX port adapter. Other types of interfaces are not affected.

  Workaround: When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Gigabit Ethernet and Fast Ethernet interfaces of all routers of the standby group.

  To prevent the symptom from occurring, remove dampening from the Gigabit Ethernet and Fast Ethernet interfaces.

- CSCse01143

  Symptoms: IPC does not function after an RPR+ switchover has occurred,

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for RPR+ and dLFIoLL.

  Workaround: Reload the microcode onto the router.

- CSCse01847

  Symptoms: When agentless hosts are allowed network access, a loss of connectivity may occur during reauthentication.

  Conditions: This symptom is observed when the host does not have a Cisco Trust Agent (CTA) configured.

  Workaround: There is no workaround.

  Further Problem Description: When an agentless host is authorized for network access, a dynamic access policy is applied for the host. This access policy is removed at the beginning of the reauthentication process, and re-applied at the end of reauthentication process. During the reauthentication process, no access policy is applied for the host. This situation may cause a disruption to network access.

- CSCse03855

  Symptoms: An IP phone display remains stuck at "Enter Number" for the duration of an outgoing call to the PSTN.

  Conditions: This symptom is observed when the IP phone runs CME version 3.3 and is connected to a BRI ISDN interface on a Cisco router that runs Cisco IOS Release 12.4. When you enable the **debug isdn q931** command, the following message is displayed in response to an outgoing setup message:

```
ISDN BR0/2/0 Q931: RX <- SETUP_ACK pd = 8  callref = 0x83
Channel ID i = 0x89
Progress Ind i = 0x8288 - In-band info or appropriate now available
```

Workaround: Prevent the Telco from sending the following information in the setup_ack message:

```
Progress Ind i = 0x8288 - In-band" information or appropriate now available
```

Note that the symptom does not occur in Cisco IOS Release 12.3(11)T10 and with CME version 3.2.

- CSCse11638

  Symptoms: A voice gateway reloads while bulk calls are being processed.

  Conditions: The symptom is observed on a Cisco voice gateway that runs VXML applications that stream voice prompts from an HTTP server.

  Workaround: Enter the **ivr prompt streamed none** command on the voice gateway.

- CSCse12154

  Symptoms: A router may crash because of a bus error when you enter the **copy scp** command to copy a configuration.

  Conditions: This symptom is observed on a Cisco router that is configured for SSH.

  Workaround: Do not use SCP. Rather, use Remote Copy Protocol (RCP) or use a TFTP transfer.

- CSCse15025

  Symptoms: An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

  When this problem occurs, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

  Because this issue impacts the signaling channels, it has been seen that calls either will not connect at all through impacted ports or in some cases when multiple simultaneous calls are present on adjacent voice ports/timeslots, the call may connect momentarily before being disconnected.

  If a problem occurs only on a single voice port, there is another problem, not this caveat (CSCse15025). PRI/BRI calls are not affected because PRI/BRI does not utilize the DSP for signaling purposes.

  When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port- number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41, and 42 is presented and some of the registers show double- octet information. See the example output (2) below.

  When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** *port- number* **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

  Further Problem Description: The changes in CSCse15025 includes changes in CSCsc11833 and CScsd90851. These changes have been shown to help mitigate this problem in the majority of cases.

There is a further detection and reset mechanism in CSCse15025 that will recover the DSP which is in this state. This mechanism will trigger immediately if the impacted voice port is an analog FXO port. For other voice ports, a delay in the detection will be present and it is possible to see the symptom of this problem before the recovery code triggers.

Note that the reset mechanism will cause any active calls utilizing the DSP in question to be dropped.

It is recommended if running with modules which can be impacted by this issue to upgrade to a release of software which contains the changes in CSCse15025. If the DSP is reset and the below output is seen, contact the TAC for further assistance. Note that this output is sent at debug level and it is recommended to enable either syslog or logging buffered on the gateway.

Logging buffered on the gateway is enabled through the global command **logging buffered 50000 debug** as an example to set the logging buffered to use 50K bytes of processor memory for logging. The output of the log can be seen with the Exec command **show log**.

Example output when detection and recovery code on gateway triggers:

```
*May 31 14:30:43.343: TDM pointers: 0100 0100 0115 0115. Deltas: 0001 0000.


*May 31 14:30:43.347: Received alarm indication from dsp(0/1)
0030 0000 0080 0000 0013 4100 2E2E 2F2E 2E2F 6D6F 6475 6C65 732F 7363 6865 6475 6C65
2F64 6562 7567 2E63 2833 3634 2900
*May 31 14:30:43.347: ../../modules/schedule/debug.c(364)


*May 31 14:30:43.347: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to Administrative Shutdown
*May 31 14:30:43.647: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to Administrative Shutdown
*May 31 14:30:43.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to Administrative Shutdown
*May 31 14:30:44.247: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to Administrative Shutdown


*May 31 14:30:48.147: Crash dump CLI may not be configured, not able to get crash
info, slot 0, dsp 1
*May 31 14:30:48.147: DSPDUMP - Recover slot 0 dsp 1
*May 31 14:30:48.147: DSPDUMP - ka sent 0, ka_cnt 51193, skip_ka 103079
*May 31 14:30:50.579: %DSPRM-5-UPDOWN: DSP 1 in slot 0, changed state to up
*May 31 14:30:50.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to up
*May 31 14:30:51.219: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to up
*May 31 14:30:51.371: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to up
*May 31 14:30:51.523: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to up
```

Following are command output examples:

1. Following is an example of normal output for FXO and EVM FXS ports.

For FXO ports, the value is usually 0x01 but for EVM FXS the value can be different. When you run the above-mentioned command, the expected output is that a single octet is displayed and only for register 39. (This command does not work for VIC-4FXS and VIC2-xFXS modules).

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x01
```

2. Following is an example of output for FXO and EVM FXS ports that indicates that the symptom has occurred. Note that the exact output for the register values is different, but when the symptom occurs, different lines with information are displayed as shown below:

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF
```

3. Following is an example of normal output for FXS and analog E&M modules. The values that are listed in a normal case may be different, but only four registers of a single octet should be displayed.

```
Values read from PEB2465 Codec connected to DSP 02 (channel 0):
------------------------------------------------------------
Extended Register Values (XR4..XR1) = 00, CC, 50, 11
```

4. Following is an example of output for FXS and analog E&M modules that indicates that the symptom has occurred.

```
Values read from PEB2x65 Codec connected to DSP 0, channel 1:
------------------------------------------------------------
Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCse16494

  Symptoms: Traffic does not flow after a Route Processor Redundancy Plus (RPR+) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 and that is configured for RPR+.

  Workaround: After the RPR+ switchover has occurred, reload microcode onto the router.

- CSCse16497

  Symptoms: A Cisco VG224 may not boot and may generate the following error message:

  ```
  ... Error : glue magic numbers do not correspond
  *** System received a Software forced crash *** ...
  ```

  Conditions: This symptom is observed on a Cisco VG224 that runs Cisco IOS interim Release 12.4(7.24)T1 but may also affect Release 12.4.

Workaround: There is no workaround.

- CSCse17175

  Symptoms: The line protocol may go down on some of the serial interfaces of a 1-port multichannel STM-1 single mode port adapter.

  Conditions: This symptom is observed on a Cisco router when the maximum number of channel groups (256) is configured on the port adapter.

  Workaround: There is no workaround.

- CSCse17317

  Symptoms: A router may during an E1R2 test for different country codes and codecs.

  Conditions: This symptom is observed on a Cisco router only when E1R2 digital semi-compelled signaling is used.

  Workaround: There is no workaround.

- CSCse22172

  Symptoms: A Cisco 3845 may crash when you enter the **copy system:running-config** command to copy the configuration to a USB flash device.

  Conditions: This symptom is observed on a Cisco 3845 that runs Cisco IOS interim Release 12.4(9.4).

  Workaround: There is no workaround.

- CSCse22900

  Symptoms: The outgoing MPLS labels for packets that are forwarded via CEF and MPLS over a BGP route may not match the labels in the BGP table.

  Conditions: This symptom is observed when there are two paths to a VPN prefix from the same egress next-hop router with different outgoing labels and when one path is a multipath candidate and the other path is not. The symptom occurs when the non-multipath candidate is withdrawn.

  Workaround: Two paths to a VPN prefix from the same egress next-hop typically indicates a provisioning error and should be avoided. When the symptom has occurred, enter the **clear ip route** command for the prefix in the VRF.

- CSCse23302

  Symptoms: A stale LDP targeted session is not removed after a session flap has occurred, which can be verified in the output of the **show mpls ldp neighbor** command.

  Conditions: This symptom is observed on a Cisco router when the LDP targeted session is removed and quickly re-added.

  Workaround: There is no workaround.

- CSCse24889

  Symptoms: Malformed SSH packets may cause a memory leak.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after malformed SSH packets have been received.

  Workaround: There is no workaround. You can reduce the number of locations that can connect to the router by using a VTY access list, as in the following example:

```
access-list 2 permit 10.1.1.0 0.0.0.255
    access-list 2 deny any
line vty 0 4
```

```
access-class 2 in
end
```

More information about configuring VTY access lists is available in the following Cisco Tech Notes: http://www.cisco.com/warp/public/707/confaccesslists.html.

- CSCse25166

  Symptoms: A traceback may be generated when you enter the **show funi pvc interface serial** *x/y* command.

  Conditions: This symptom is observed on a Cisco router when a null data structure is accessed.

  Workaround: There is no workaround.

- CSCse25331

  Symptoms: After upgrading the Cisco IOS on a Cisco 7200 series router that is using a PA-A3-IMA, shaping accuracy problems can be observed. The PVC is shaped at a rate bigger than the configured value.

  Conditions: This problem is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCse34097

  Symptoms: When a voice call is made to one of the busy channels of BRI/PRI port, the call gets rejected and then another call is made to the available port. The call gets connected, and the user hears an annoying hissing sound.

  Conditions: The procedure to recreate this scenario is the following:

  ```
  Phone a & b ---OGW --VoIP --TGW(2611) --BRI/PRI --PBX -- phone c & d
  Phone a calls phone c;
  Phone b calls phone c;
  Phone b calls phone d;
  ```

  Phone d picks up and hears a hissing noise.

  Workaround: There is no workaround.

- CSCse35588

  Symptoms: Performance degrades when you add the **inspect dns** keywords in the Firewall policy table.

  Conditions: This symptom is observed when on a Cisco router and occurs because the **inspect dns** keywords use the old IDS code.

  Workaround: Do not add the **inspect dns** keywords. Rather, add the **udp** keyword in the Firewall policy table.

- CSCse39330

  Symptoms: A router does not boot when you first enter the **secure boot-image** command followed by the **format disk** command and then you use the secure image to attempt to boot the router.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCse39452

  Symptoms: OGW rejects incoming OLC from an alternate endpoint when the slow start procedure is used and so the call is rejected.

Conditions: This symptom has been observed when OGW is configured to use the slow start procedure.

Workaround: There is no workaround.

Further Problem Description: OGW is configured to use the slow start procedure. OGW receives alternate endpoints in the ACF. The call on the primary endpoint fails after H.245 procedures are completed and logical channel are opened. Now OGW tries the call on alternate endpoint, but it rejects the incoming OLC from the alternate endpoint, thus resulting in call failure.

- CSCse42444

  Symptoms: When you run and monitor the cbQosCMDropPkt MIB variable, the counters may become stuck while the command line is growing properly. When you run and monitor the cbQosPoliceExceededPkt MIB variable, both counters report the same value.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(15)T13 but may also affect Release 12.4.

  Workaround: There is no workaround.

- CSCse42951

  Symptoms: A spurious memory traceback may be generated during Certificate Authority (CA) enrollment.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.9)T but may also affect Release 12.4.

  Workaround: There is no workaround.

- CSCse42991

  Symptoms: A memory leak may occur in the CEF Scanner process of a Cisco 7200 VXR router that has an NPE-G1 processor when a virtual-template interface is configured to perform CEF load balancing on a per-packet basis instead of a per-destination basis.

  Conditions: This symptom is observed on a 7204VXR that functions as an LNS and that runs the c7200-js-mz image of Cisco IOS Release 12.3(15) or the 7200-js-mz image of Cisco IOS Release 12.3(19). The symptom may also occur in other releases.

  Workaround: Use the default CEF load balancing on a per-destination basis. If you need to configure loadbalancing on a per-packet basis, disable IP CEF accounting by entering the **no ip cef accounting per-prefix non-recursive** command.

- CSCse43066

  Symptoms: A Cisco Multiservice IP-to-IP Gateway (IPIPGW) may crash while functioning under stress.

  Conditions: This symptom is observed on a Cisco IPIPGW that runs Cisco IOS interim Release 12.4(9.4) or interim Release 12.4(9.9)T.

  Workaround: Configure slow start:

  ```
  voice service voip
  h323
  call start slow
  ```

  Note that the symptom does not occur in releases earlier than interim Release 12.4(9.4) or interim Release 12.7(7.24)T.

- CSCse44240

  Symptoms: No call may come up on a Cisco AS5400 or Cisco AS5850. The debug shows that DSP calls fails. Calls on SS7-H.323-SS7 legs and H.323-SS7-H.323 legs fail. (Setup calls on PRO-H.323-PRI legs are successful.)

  Conditions: These symptoms are observed on a Cisco AS5400 and Cisco AS5850 that run Cisco IOS interim Release 12.4(9.11) in either an IUA or RLM configuration. The symptoms occur only when the originating gateway runs Release 12.4(9.11); the symptoms do not occur when both the originating and terminating gateways run Release 12.4(9.11).

  Workaround: There is no workaround.

- CSCse45425

  Symptoms: A VAM2 may reset when it receives a malformed ESP packet, and a "Free Pool stuck" error message may be generated. This situation causes high CPU usage in the encryption process while the software is handling the encryption as opposed to the hardware. Even when the VAM2 recovers, the high CPU usage remains because the software-encrypted tunnels do not fall back to hardware encryption until the SA lifetime expires.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(19) or Release 12.4(7a).

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred and after the VAM2 has recovered, disable software encryption by entering the **no crypto engine software ipsec** command to force the encryption back to the hardware.

- CSCse46908

  Symptoms: A router may crash when you configure an IPv6 interface with a policy route map.

  Conditions: This symptom is observed on a distributed platform when you first configure an IPv6 interface with an access control list (ACL) with a very long name and then configure a policy route map with a very long name.

  Workaround: Do not use very long names for ACLs and policy route maps.

- CSCse48814

  Symptoms: A router crashes when you enter the **ip nat outside** interface configuration command on an interface.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim Release 12.4(9.13) or interim Release 12.4(09.19a) and that is configured for Network Based Application Recognition (NBAR).

  Workaround: There is no workaround.

- CSCse48847

  Symptoms: A router that functions as a Home Agent (HA) may crash while it processes an AAA response and sends it back to the Mobile Node (MN) via a tunnel that is established between the HA and a Foreign Agent (FA). The symptom occurs because the memory stack becomes low on the HA.

  Conditions: This symptom is observed on a Cisco router that functions as an HA and that runs Cisco IOS interim Release 12.4(9.13).

  Workaround: There is no workaround.

- CSCse49985

  Symptoms: A software-forced crash may occur on a Cisco 3745, and an error message similar to the following may be displayed:

  ```
  rcojx67-vgw01-3745 uptime is 1 day, 16 hours, 19 minutes
  ```

```
System returned to ROM by error - a Software forced crash, PC 0x60A87D38 at 15:59:36
GMT Tue May 16 2006

System restarted at 16:00:35 GMT Tue May 16 2006

System image file is "flash:c3745-ipvoice-mz.123-14.T3.bin"
```

Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(14)T3 only when there are some memory allocation failures. The symptom may also affect Release 12.4.

Workaround: There is no workaround.

- CSCse50445

  Symptoms: A router that is configured for AutoQoS may crash when the stack for the Exec process is running low.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) or interim Release 12.4(09.19a).

  Workaround: Enter the **ip nbar protocol-discovery** command.

- CSCse52987

  Symptoms: The line protocol on a newly configured SRP interface may remain down and does not come up after you have entered the **no shutdown** command.

  Conditions: This symptom is observed on a Cisco router that has an SRP/DPT port adapter.

  Workaround: There is no workaround.

- CSCse53224

  Symptoms: All of the (six) processors on a Multiprocessor WAN Application Module (MWAM) crash and reload continuously, causing the MWAM to remain inaccessible.

  Conditions: This symptom is observed on an MWAM that is installed in a Cisco Catalyst 6500 series or Cisco 7600 series and that runs Cisco IOS interim Release 12.4(9.9) or a later release.

  Workaround: There is no workaround.

- CSCse55522

  Symptoms: A Versatile Interface Processor (VIP) with CT3 PA crashes continuously.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS interim Release 12.4(9.9).

  Workaround: There is no workaround.

- CSCse55652

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

  Conditions: This symptom is observed on a distributed router such as a Cisco AS5850 or Cisco 7500 series that runs Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCse56129

  Symptoms: On a Cisco VG224 that is manufactured in May 2006 or later and that contains the new analog codec for the onboard analog FXS voice port, a voice port that is registered to a CallManager Express that runs Cisco IOS Release 12.4(4)XC may incorrectly detect a hookflash when a call is being picked up.

  Conditions: This symptom is observed when, during the call pick-up, the CME sends an onhook to the port of the Cisco VG224, presents a new call, and immediately instructs the port to enter the connected state. During this sequence of events, the voice port on the Cisco VG224 incorrectly reports a hookflash. Note that the symptom may also occur in Release 12.4 or Release 12.4T.

Workaround: Enter the **no supervisory disconnect lcfo** command for the voice port of the Cisco VG224.

Further Problem Description: To find out whether or not the Cisco VG224 has the new analog codec installed, enter the **show version** command and look in the output for the following:

```
On-Board Twenty-Four FXS Analog Voice Module V2.1
```

A Cisco VG224 that does not have the new analog codec installed shows the following in the output of the **show version** command:

```
On-Board Twenty-Four FXS Analog Voice Module V1.3
```

- CSCse56660

  Symptoms: Inbound calls to FXO ports on Cisco IOS VoIP gateways connect, but audio is not present.

  Conditions: With **caller-id enable** configured on FXO ports, the call will connect, but no audio is heard. When this occurs, the following error message can be seen at debug level:

  ```
  Jun 20 01:41:15.855: mbrd_e1t1_vic_connect: setup failed
  Jun 20 01:41:15.855: flex_dsprm_tdm_xconn: voice-port(0/0/1), dsp_channel (/0/2/0)
  ```

  Workaround: Disable caller id on the voice-port.

- CSCse59775

  Symptoms: A Cisco 3845 that is configured for voice may reload because of a software-forced crash that is caused by a Redzone memory corruption.

  Conditions: This symptom is observed on a Cisco 3845 that runs Cisco IOS interim Release 12.4(9.15).

  Workaround: There is no workaround.

- CSCse63494

  Symptoms: A router that is configured for Real-Time Protocol (RTP) may generate CPUHOG events and a traceback similar to the following:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (951/33),process = VOIP_RTCP.
  -Traceback= 0x60EA5A78 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  ```

  Alternatively, the router may unexpectedly reload and generate the following error message and traceback:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = VOIP_RTCP. -
  Traceback= 0x60EA5A58 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  %Software-forced reload
  Preparing to dump core...
  ```

  Conditions: This symptom is observed on a Cisco router that receives a badly formatted RTP Control Protocol (RTCP) packet.

  Workaround: There is no workaround.

  Further Problem Description: Typically, the badly formatted RTCP packet is produced by a device that does not conform to the RFC 3550 standard.

- CSCse68355

  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

- CSCse79884

  Symptoms: You may not be able to exit the **session** command.

  Conditions: This symptom is observed on MWAM line card processors that are installed in a Cisco Catalyst 6500 series switch or a Cisco 7600 series router.

  Workaround: If the **session** command is executed via a Telnet session to the supervisor engine: log in to the supervisor engine via its console to find out the line number in the output of the **show user** command that corresponds to the processor that is unable to exit from the **session** command. Look for IP address 127.0.0. <slot> <processor number used for session> to find the line number. Then, enter the **clear line** *line number* command to clear the session.

  If the **session** command is executed from the MWAM console itself (which is stuck), there is no workaround.

- CSCse85329

  Symptoms: When you re-insert a PA-MC-8TE1+ port adapter in the same slot of a Cisco 7200 series via an OIR, the serial interface may enter the Down/Down state. When you enter the **shutdown** command followed by the **no shutdown** command on the T1 or E1 controller, the serial interface may transition to the Up/Down state, still preventing traffic from passing.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(7) or a later release.

  Workaround: Reload the router.

- CSCse89105

  Symptoms: RADIUS packets may be dropped or extra memory may be allocated when RADIUS packets are sent.

  Conditions: These symptoms are observed on a Cisco platform that is configured for SSG when a RADIUS packet with a length of more than 1024 bytes is sent.

  Workaround: There is no workaround.

- 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

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

  Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third-party system.

  Workaround: There is no workaround.

Terminal Service

- CSCej00344

  Symptoms: A router that is configured for X.25 routing may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T2 with an X.25-over-TCP (XOT) configuration. The symptom may also affect Release 12.4 and Release 12.4T.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek28604

  Symptoms: A Cisco AS5400 reloads unexpectedly because of a memory leak in the ISDN L2 process.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.4(7) and that functions in a call manager-backhaul configuration after running under stress for about 24 hours.

  The output of the **show processes memory** command, collected in regular intervals, shows a memory leak in the ISDN L2 process. The amount of memory that is held by the ISDN L2 process is very large, and the amount of free processor memory is small when the router reloads unexpectedly. This symptom is not observed on a Cisco AS5850, but may also occur on this platform when it runs under stress for more than 24 hours.

  Workaround: Enter the **isdn k 1** command on all backhauled serial interfaces.

- CSCek40618

  Symptoms: A router may crash by address error (load or instruction fetch) exception during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCin98788

  Symptoms: When a BBA group that is associated with a live PPPoE session is removed, the session is not cleared.

  Conditions: This symptom is observed with either a named or a global BBA group.

  Workaround: There is no workaround.

- CSCsd19867

  Symptoms: BRI interfaces does not come up when you reload a router. You must enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected BRI interfaces to bring them up.

  Conditions: This symptom is observed when you enter the **no isdn spoofing** command and reload the router.

  Workaround: Disable the **no isdn spoofing** command.

- CSCsd38761

  Symptoms: A router may crash when the AAA per-user attribute idletime is specified in the user profile.

  Conditions: This symptom is observed on a Cisco router that is configured for PPP and AAA.

  Workaround: Do not specify the AAA per-user attribute idletime in the user profile.

- CSCsd72854

  Symptoms: When IS-IS is configured on an MLP interface of a 6-port channelized T3 Engine 0 line card, the line card may fail to come up because PPP fails to negotiate OSICP on the MLP interface.

  Conditions: This symptom is observed on a Cisco 12000 series router after you have reloaded the router.

  Workaround: Increase the PPP timeout retry interval to 10 seconds by entering the **ppp timeout retry** *10* command on the interface. (The default timeout retry interval is 2 seconds).

- CSCsd74130

  Symptoms: When an HSSIRSET, SERRSET, or FDDIRSET error message is generated or when the output becomes stuck, a VIP does not come up during its first recovery attempt.

  Conditions: This symptom is observed on a Cisco platform that is configured with a VIP when a CCB timeout occurs during an IDB reset or when the output becomes stuck.

  Workaround: There is no workaround.

- CSCsd81350

  Symptoms: When asynchronous serial interfaces are used as member links in multilink PPP bundles, the router may crash due to memory corruption.

  Conditions: This problem can occur under conditions where multilink fragmentation is done, and where the bundle includes at least one member link that is an asynchronous interface.

  Workaround: Disable fragmentation on the bundle interface for any bundle that may include asynchronous links as members. Alternatively, if the use of multilink is not a requirement, disable multilink on the asynchronous interfaces.

- CSCse05777

  Symptoms: A router may reload unexpectedly when you configure more multilink interfaces than the maximum number that the router can support. The router should not reload but should generate an error message.

Conditions: This symptom is observed on any Cisco router that imposes a limit on the number of multilink interfaces.

Workaround: Do not exceed the maximum number of multilink interfaces.

- CSCse16539

  Symptoms: VPDN loadbalancing incorrectly biases to one LNS (IP address) instead of sharing the session load between the different LNSs after LNS return from the busy list.

  Conditions: This occurs when multiple LNSs are configured for one vpdn-group and are unreachable. They are moved to the busy list. Once the LNSs become reachable again, this problem occurs.

  Workaround: There is no workaround.

- CSCse19642

  Symptoms: The ISDN Layer-2 status may become “TEI_ASSIGNED” and may remain in this state even when you enter the **clear interface** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4, Release 12.4(2)XA1, or Release 12.4(6)T and occurs under the following conditions:

  – X.25 is configured on a D channel for use in Japan with an ISDN carrier.
  – Both the B channel and D channel are used.
  – The **clear interface bri 0** command is enabled.
  – In Layer-2 sequence, the router receives an “SABMEp” message irregularly between “IDREQ” and “IDASSN” messages from the ISDN switch.

  Workaround: Reload the router.

  Alternate Workaround: Disconnect and connect the cable on the U reference point (between the Telco and the DSU) and enter either one of the following command combinations instead of the **clear interface bri 0** command:

  – The **clear interface bri 0:0** and **clear interface bri 0:1** commands.
  – The **clear interface bri 0:0** and **clear interface bri 0:2** commands.

- CSCse45182

  Symptoms: When a PPPoE server receives a second PADI from a client (that is, a PADI with the same unique client ID), the PPPoE server may send a PADS with an unknown MAC address.

  Conditions: This symptom is observed on a Cisco platform that functions as a PPPoE server that has established a PPPoE session with a client and occurs while PPP LCP negotiation is in progress.

  Workaround: There is no workaround.

- CSCse64924

  Symptoms: A router crashes when you configure a Frame Relay PVC bundle with Frame Relay FRF.9 payload compression.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.15)T but may also affect other releases.

  Workaround: There is no workaround.

- CSCse71875

  Symptoms: A router may crash when you enter the **frame-relay inverse-arp ip** *dlci* command.

  Conditions: This symptom is observed when you attempt to configure a hunt-group member.

Workaround: Do not enter the **frame-relay inverse-arp ip** *dlci* command. Rather, configure the hunt-group master dialer interface.

- CSCse78652

  Symptoms: The queuing mode on Multilink interfaces is erroneously defaulting to fair queuing instead of FIFO. This is causing distributed Cisco Express Forwarding (dCEF) to fail on Cisco 7500 routers.

  Conditions: This symptom happens on all Multilink interfaces.

  Workaround: There is no workaround.

- CSCse79994

  Symptoms: BRI Layer 2 remains in the ESTABLISH_AWAITING_TEI state instead of entering the MULTIPLE_FRAME_ESTABLISHED state.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(8d)

Cisco IOS Release 12.4(8d) is a rebuild release for Cisco IOS Release 12.4(8). The caveats in this section are resolved in Cisco IOS Release 12.4(8d) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCse66080

  Symptoms: A memory leak may occur in the Entity MIB API process.

  Conditions: This symptom is observed when an entity is registered with the same name as an entity that is already registered.

  Workaround: There is no workaround.

- CSCsf32390

  Symptoms: When tuning particle clone, F/S, and header pools after these were made configurable via CSCuk47328, the commands may be lost on a reload.

  Conditions: If the device is reloaded the commands are not parsed on a reload and this results in the defaults being active. This may result in traffic loss if the increased buffers were needed to enable greater forwarding performance for the specific network design.

  Workaround: Configure an applet to enter the buffer values again after a reload. A sample applet would be:

```
event manager applet add-buffer
 event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 3.0 cli command "buffers particle-clone 16384"
 action 4.0 cli command "buffers header 4096"
 action 5.0 cli command "buffers fastswitching 8192"
 action 6.0 syslog msg "Reinstated buffers command"
```

- CSCsg21398

  Symptoms: The Cisco IOS software image may unexpectedly restart when a crafted "msg-auth-response-get-user" TACACS+ packet is received.

  Conditions: This symptom is observed after the Cisco platform had send an initial "recv-auth-start" TACACS+ packet.

  Workaround: There is no workaround.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  – You reload the router.

  – A switchover of the active RP occurs.

  – You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- 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 whenever 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 a Cisco IOS software 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.

IP Routing Protocols

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- CSCek47667

  Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

  Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsg00860

  Symptoms: Enabling NAT outside on the public interface terminates the VPN connection as GREoverIPSEC. Inbound ACL applied on the public interface starts to drop decrypted GRE traffic.

  Conditions: This symptom has been observed with the use of IP NAT outside on the public VPN interface.

  Workaround: There are 2 workarounds:

  1. Configure NAT translations for all traffic, to force NAT processing on the packet even if no address will actually be translated. Example:

     ```
     ip nat inside source static 172.16.68.5 172.16.68.5
     ```
     It is not a scalable workaround but may work for some deployments.
  2. Configure an additional ACL entry in the inbound access-list to permit the incoming GRE traffic.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

Workaround: There is no workaround.

- CSCsh80678

  Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(22) or a later release when the **auto-summary** command is enabled for BGP.

  Workaround: Enter the **no auto-summary** command.

- CSCsh90153

  Symptoms: Connectivity is lost through a router when traffic is processed twice by NAT.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(8a), that is configured for NAT and PBR, and that has a firewall feature enabled. Under certain conditions, traffic is processed twice by NAT when it does not need to be.

  Workaround: Remove the firewall configuration from the router.

  Further Problem Description: Syslogs and the output of the **show ip nat translation** command show that traffic that is processed twice by NAT does not traverse the router.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

  Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  Workaround: Add area 0 in the OSPF VRF processes.

  Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

Miscellaneous

- CSCds25257

  Symptoms: A gatekeeper rejects new registration requests from a Cisco Unified CallManager (CUCM) or other H.323 endpoints with Registration Rejection (RRJ) reason of duplicateAlias. Attempting to clear this stale registration fails and a “No such local endpoint is registered, clear failed.” error message is generated.

  Conditions: This symptom is observed in the following topology:

  CUCM H.225 trunks register to a gatekeeper (GK) cluster. Gatekeeper 1 (GK1) and gatekeeper 2 (GK2) are members of the GK cluster. The CUCM registers first to GK1, then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

  When the H.225 trunk attempts to register with GK1, it is rejected because the alternate registration is still present, and there is no way to clear it.

```
10.9.20.3       34273 10.9.20.3       32853 SJC-LMPVA-GK-1    H323-GW A
    ENDPOINT-ID: 450FC24400000000  VERSION: 5  AGE: 1618993 secs
SupportsAnnexE: FALSE
    g_supp_prots: 0x00000050
    H323-ID: SJC-LMPVA-Trunk_4
```

  Workaround: Reset the gatekeeper by entering the **shutdown** command followed by the **no shutdown** command, or reboot the affected GK.

- CSCed57504

  Symptoms: A router that is configured with a virtual template may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router on which a session that uses a virtual-template is terminated and occurs when the session is cleared from a DSL CPE router that is the peer router for the connection.

  Workaround: There is no workaround.

- CSCek38201

  Symptoms: A router may reload or display an alignment traceback when you enter the **show crypto socket** command.

  Conditions: This symptom is observed on a Cisco router that has an OSPFv3 IPSecv6 configuration.

  Workaround: There is no workaround. To prevent the symptom from occurring, do not enter the **show crypto socket** command in an OSPFv3 IPSecv6 configuration.

- CSCek45344

  Symptoms: A Cisco AS5400XM gateway crashes after 24 hour stress with E1-R2 calls.

  Conditions: This symptom occurs in stress conditions after a period of 24 hours.

  Workaround: There is no workaround.

- CSCek47653

  Symptoms: A voice gateway may crash because of a bus error that is related to an MGCP Visual Message Waiting Indicator (VMWI) function.

  Conditions: This symptom is observed on a Cisco IAD 2430 that runs Cisco IOS Release 12.3(14)T2. The symptom may also affect Release 12.4 and Release 12.4T.

  Workaround: There is no workaround.

- CSCek48251

  Symptoms: When you enter the **redundancy switch-activity force** command on the active eRSC of a Cisco AS5850 while incoming VoIP H.323 calls and outgoing CAS calls are being processed, the standby eRSC does become the active eRSC and processes the calls but soon afterwards may crash at "csm_enter_idle_state."

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(9)T and that functions in RPR+ mode. The symptom may also affect Release 12.4.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRI calls are being processed.

- CSCek55486

  Symptoms: The native Gigabit Ethernet (GE) interface on an NPE-G1 card may reset unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series when the underrun counter for the native GE interface increments continuously. You can verify the underrun counter in the output of the **show interfaces gigabitethernet** *slot/port* command.

  Workaround: There is no workaround.

- CSCek64188

  Symptoms: An error message indicating memory leak and pending transmission for IPC messages is displayed as follows:

  ```
  *Dec  3 01:31:31.792: %IPC-5-WATERMARK: 25642 messages pending in xmt for the
  port Primary RFS Server Port(10000.C) from source seat 2150000
  *Dec  3 01:32:01.489: %SYS-2-MALLOCFAIL: Memory allocation of 4268 bytes
  failed from 0x9F32944, alignment 32
  ```

  Conditions: This issue is triggered by CSCeb05456 and is applicable only if your Cisco IOS image has integrated the fix of CSCeb05456.

  Workaround: Periodically, reload the router so that the IPC buffer pool will be reinitialized.

- 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.

- CSCsd28214

  Symptoms: A Cisco router may crash because of a watch dog timeout while running the RIP routing protocol.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3(19) when an interface changes state at the exact same time that a RIP route that was learned on this interface is being replaced with a better metric redistributed route. For example, when RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0 interface and then RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, the RIP route is removed. However, when during this time the Fast Ethernet 1/0 interface goes down, the router may crash because of a watch dog timeout. Note that the symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCsd34529

  Symptoms: A Cisco router may crash when a policy map is simultaneously displayed and unconfigured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T but may also affect Release 12.4. The symptom occurs when the **show policy-map** command is entered via one CLI session while the **no policy-map** *policy-map-name* command is entered via another CLI session.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  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.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587

- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM) CSCsi97695

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

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

Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.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.

- CSCse18355

  Symptoms: A Cisco AS5850-ERSC gateway reboots continuously with the message:

```
Bundled Rommon and FPGA versions are different from
 the current system version. Updating the system.
 This might take a while

 System reload is required before upgrade can be done.
 Rebooting the system ..
 !
```

  Conditions: This symptom has been observed when a Cisco AS5850-ERSC gateway is running Cisco IOS interim Release 12.4(7.24)T.COMP.

  Workaround: Boot to ROM monitor mode and enter the following commands:

```
SKIP_UPGRADE=1
sync
```

  This step skips the upgrade process. To revert back, enter the following commands:

```
unset SKIP_UPGRADE
sync
```

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1
end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any

line vty 0 4
access-class 99 in
end
```

Further Problem Description:

For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6350_TSD_Products_Configuration_Guide_Chapter.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- CSCse75920

  Symptoms: A Cisco router experiences a memory leak for the processes SCCP application and Chunk manager.

  Conditions: The symptom has been observed after configuring the router for MTP and transcoding.

  Workaround: There is no workaround.

- CSCse91102

  Symptoms: A Cisco IAD 2430 IAD crashes on Cisco IOS Release 12.4(4)T2. Traceback decodes indicate memory corruption. The following events may also appear in the log:

```
%SYS-3-BADMAGIC: Corrupt block at
%SYS-6-MTRACE: mallocfree: addr, pc
%SYS-6-BLKINFO: Corrupted magic value in in-use block
%SYS-6-MEMDUMP:
```

Conditions: The router crashes where the decodes indicate check heaps as the source with any or all of the following also included in decode:

```
crashdump
validblock
validate_memory
checkheaps
checkheaps_process
```

Workaround: There is no workaround.

- CSCsf08998

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

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

- CSCsg07907

  Symptoms: A Cisco 3845 router unexpectedly reloads with bus error as seen in the show version when enabling DSP mini logger (voice dsp <slot> command history enable).

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4 with conferencing enabled on the DSP slot that minilogger is being turned on for.

  Workaround: Disable conferencing on that slot, if possible.

- CSCsg15598

  The Intrusion Prevention System (IPS) feature set of Cisco IOSÆ contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml

- CSCsg18933

  Symptoms: A RIP route is learned from a RIP neighbor via a dialer interface (or other virtual interface type). When the neighbor disconnects and the interface goes down, the RIP route is removed from the RIP database. However, the RIP route remains in the routing table.

  Conditions: - RIP is configured with the **no validate-update-source** command. - RIP routes are learned via a virtual interface. - The virtual interface is using a negotiated address. - The problem is platform-independent.

  Workaround: Use the **clear ip route** command to remove the affected routes from the routing table.

- CSCsg28628

  Symptoms: NAS pkg asynchronous calls fail after a redundancy switchover has occurred, and the following error message is generated:

  Modems unavailable

  Conditions: This symptom is observed on a Cisco AS5850 that functions in RPR+ mode. This situation may impact service.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **redundancy switchover** command a couple of times to restore the Cisco AS5850 to normal operation.

- 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.

- CSCsg59326

  Symptoms: When an ATM (that is, a cash machine, not a WAN platform) is connected to a switch service module, significant packet loss may occur.

  Conditions: This symptom is observed on a Cisco 2800 series router.

  Workaround: Change the Ethernet speed to 10 Mbps at both ends.

- 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.

- CSCsg76715

  Symptoms: A device crashes when you delete an ACE that was inserted in the middle of the ACL rather than added at the end of the list.

  Conditions: This symptom is observed when all of the following conditions are present:

  - The inserted ACE has a destination prefix length of 0, that is, is has an “any” statement instead of a destination address.
  - The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an “any” statement), and the inserted ACE has a lower sequence number than this other ACE.
  - The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

  Workaround: First, delete the inserted ACE. Then, delete the other ACE with the same SRC prefix length and an destination prefix length that is greater than 0.

  Alternate Workaround: Delete the complete ACL.

- CSCsg96319

  Symptoms: When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:***number ip-address* command.

  Conditions: This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhanmt_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  Workaround: Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- CSCsg99814

  Symptoms: On a router that functions in a GRE over IPSec or Virtual Tunnel Interface (VTI) configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface.

  Conditions: This symptom is observed when the ACL on the tunnel interface is configured on the outbound physical interface on which the IPSec tunnel is terminated.

  Workaround: Apply the outbound ACL on the protected LAN interface instead of on the tunnel interface.

- CSCsh33430

  Symptoms: A traceback may occur in an HSRP function and the platform may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that has the HSRP Support for ICMP Redirects feature enabled and occurs when a learned HSRP group is removed after a resign message has been received.

  Workaround: Disable the Support for ICMP Redirects feature by entering the **no standby redirects** global configuration command.

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

  ```
  %MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of [dec] - VRF
  [chars]
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

  Workaround: There is no workaround.

- CSCsh58082

  Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

  There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

  Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsh75827

  Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the "J" Service-Info attribute), has logged out from the SESM, and then renews its IP address.

  Workaround: There is no workaround.

- CSCsh94526

  Symptoms: When an acct-stop message is received for a non-RADIUS proxy user (that is, a normal IP user), a router that is configured for SSG crashes.

  Conditions: This symptom is observed when SSG is configured for RADIUS proxy mode and when the **ssg wlan reconnect** command is enabled.

  Workaround: There is no workaround.

- CSCsh97579

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi27540

  Symptoms: A VSI session may become stuck in the "RESYNC_UNDERWAY" state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

  Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

  Workaround: There is no workaround.

- 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.

- CSCsi67763

  The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

  http://www.kb.cert.org/vuls/id/739224

  By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

  Cisco response is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml

- CSCsi84017

  Symptoms: When you reload a Cisco 2600 series, the router may hang.

  Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

  Workaround: There is no workaround.

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.

Wide-Area Networking

- CSCek59078

  Symptoms: An L2TPv3 session is established when voluntary tunneling is configured and both peers have corresponding configurations. However, after you configure a pseudowire on a virtual PPP interface on one of the peers, the session on this peer is up but the line protocol is down, an a "virtual-PPP1 is up, line protocol is down" error message is generated.

  Conditions: This symptom is observed when the virtual PPP interface is first deleted via the **no interface virtual-ppp** *number* command and then reconfigured via the **interface virtual-ppp** *number* command before you configure a pseudowire on the virtual PPP interface.

  Workaround: Before you configure a pseudowire on the virtual PPP interface, ensure that the virtual PPP interface has never been unconfigured via the **no interface virtual-ppp** *number* configuration command.

- CSCsb24255

  Symptoms: A router may generate the following error message and a MALLOC failure may occur:

  ```
  flex_dsprm_voice_connect: voice tdm connect failed
  ```

  Conditions: This symptom is observed on a Cisco router that processes a large number of calls with a short call duration via an E1 PRI.

  Workaround: There is no workaround.

- CSCsc39890

  Symptoms: A router that is running Cisco IOS may reload unexpectedly.

  Conditions: For this symptom to occur, the router must be configured for ISDN. One possible trigger is when using SNMP to poll information about calls while the calls are in the process of completing.

  Workaround: There is no workaround.

- CSCsf30493

  Symptoms: When a T.37 onramp call is made, the following error message may be generated:

  ```
  %CSM-3-NO_VDEV: No modems associated
  ```

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS interim Release 12.4(10.7). The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCsh06841

  Symptoms: A router may crash while establishing a PPP session.

  Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

  Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsh82513

  Symptoms: The output of the **show isdn active** command may show disconnected calls.

  Conditions: This symptom is observed on a Cisco router when analog modem calls are made after a normal ISDN digital call has been made.

  Workaround: There is no workaround.

- CSCsi74960

  Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

  Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

  Workaround: There is no workaround.

- CSCsj10593

  Symptoms: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(15.6) and that functions as a TGW with all PRI switch types from the user to the network side. The symptom occurs when the **isdn test call interface** *interface-number dialing-string* command is entered at the platform on which the call is initiated, when the originating gateway (OGW) is configured for the National ISDN (primary-ni) switch type, and when the TGW is configured for the NT DMS-100 (primary-dms100) switch type. The symptom may also affect Release 12.4T.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(8c)

Cisco IOS Release 12.4(8c) is a rebuild release for Cisco IOS Release 12.4(8). The caveats in this section are resolved in Cisco IOS Release 12.4(8c) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsf19139

  Symptoms: %RADIUS-3-NOSERVERS messages are logged after a reload in Cisco IOS Release 12.3(18). At this time, the RADIUS accounting tickets are not generated.

  Conditions: This symptom has been observed on a Cisco AS5300 gateway.

Workaround: Enter into configuration mode and change the order of the servers under the server group.

- CSCsg03830

  Symptoms: The **tacacs-server directed-request** command appears in the running configuration when is should be disabled. When you disable the command by entering **no tacacs-server directed-request** and reload the router, the command appears to be enabled once more.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for CSCsa45148, which disables the **tacacs-server directed-request** command by default.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa45148. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Temporary Workaround: Each time after you have reloaded the router, disable the command by entering **no tacacs-server directed-request**.

Miscellaneous

- CSCek55511

  Symptoms: A Cisco AS5400HPX that is running Cisco IOS Release 12.3(11)T7 may crash with IO Memory corruption.

  Conditions: The crash may occur when polling for ccrpCPVGEntry, and resource pooling is enabled on the Gateway.

  Workaround: Disable SNMP polling for ccrpCPVGEntry.

- CSCsd50476

  Symptoms: A serial link goes down.

  Conditions: This symptom occurs when a T1/E1 controller that is configured with channel-group causes the serial link to go down. The CEM interface will not come up.

  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.

- CSCse03855

  Symptoms: An IP phone display remains stuck at “Enter Number” for the duration of an outgoing call to the PSTN.

  Conditions: This symptom is observed when the IP phone runs CME version 3.3 and is connected to a BRI ISDN interface on a Cisco router that runs Cisco IOS Release 12.4. When you enable the **debug isdn q931** command, the following message is displayed in response to an outgoing setup message:

  ```
  ISDN BR0/2/0 Q931: RX <- SETUP_ACK pd = 8  callref = 0x83
  Channel ID i = 0x89
  Progress Ind i = 0x8288 - In-band info or appropriate now available
  ```

  Workaround: Prevent the Telco from sending the following information in the setup_ack message:

  ```
  Progress Ind i = 0x8288 - In-band" information or appropriate now available
  ```

  Note that the symptom does not occur in Cisco IOS Release 12.3(11)T10 and with CME version 3.2.

- CSCse42141

  Symptoms: T38 fax calls fail when they come inbound through DID Analog ports. In the debug h245 asn1, there is no OLCAck sent back towards the fax server.

  Conditions: This symptom was only reproduced on analog ports. PRI works with the same configuration.

  Workaround: Send the fax call through a PRI.

- CSCse89373

  Symptoms: A second PRI link gets deactivated, with no ability to process incoming and outgoing calls, when the second one is remotely, physically, manually (CLI command) deactivated.

  Conditions: This symptom occurs when the first PRI is type primary-net5, and the second PRI is type primary-qsig. Deactivate the second PRI remotely or locally by physically disconnecting the cable or issuing the **shutdown** command under the corresponding E1 controller.

  Workaround: There is no workaround.

- CSCsf03412

  Symptoms: The **boot flash** command or the boot TFTP crashes a router.

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Interim Release 12.4(7.24)T.

  Workaround 1: Use the boot flash:<image name> instead of boot flash <imagename> command
  Workaround 2: Use Cisco IOS Release 12.3(11)T.

Workaround 3: Copy the image to flash and use the boot flash:<imagename> command, if the boot TFTP is the problem.

- 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

- CSCsf31178

  Symptoms: HWIC-1GE-SFP may experience an issue where the Gig Ethernet interface is “stuck” in a Line UP/Protocol Down state. While in this state, the interface will not pass traffic. Clearing the interface or manually disabling/enabling will clear the condition. This symptom does not occur when 1000BASE-T SFP is used.

  Conditions: A Loss of Signal (for example, unplugging the cable) may cause the interface to become stuck in a Line UP/Protocol Down state.

  Workaround: Clearing the interface or manually shutting it down, then bringing it back up will clear the problem.

- CSCsf95938

  Symptoms: There is a leak in middle buffers after all Onboard DSPRM Pools are depleted.

  Conditions: This symptom is observed on a Cisco 3800 series router that is running Cisco IOS Release 12.4(7b) with support for CVP survivability.

  Workaround: There is no workaround.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsg05350

  Symptoms: A Cisco AS5850 crashes due to a chunk memory leak. See the following:

  Sep 9 13:07:04.428: %DSMP-3-INTERNAL: Internal Error : NO MEMORY

  ```
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  Sep  9 13:07:04.468: %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  Sep  9 13:07:04.744: %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a
  reload due to Fragmented processor_memory, Free processor_memory = 10402472 bytes,
  Largest processor_memory block = 522632 bytes
  ```

  Conditions: This symptom occurs when there is a chunk memory leak.

  Workaround: There is no workaround.

- CSCsg11718

  Symptoms: A VRF may become stuck in the “Delete Pending” state.

Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- 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.

- CSCsg69205

  Symptoms: On a Cisco PE router, "ip flow egress" configured on the PE-CE link does not capture traffic streams destined for the CE router.

  Conditions: This symptom occurs when the MPLS interface is a multilink interface.

  Workaround: Configure "mpls netflow egress" on the interface towards the CE. Afterwards, this command can be removed, and the traffic is still captured by netflow.

Wide-Area Networking

- CSCir00712

  Symptoms: On Cisco LAC software running Cisco IOS Release 12.3(14)T, when the fragmented data traffic is received on the LAC over the L2TP tunnel, the IP layer reassembles the packet and routes the packet on the wrong interface instead of consuming the L2TP data traffic locally.

  Conditions: This symptom has been seen when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel.

  Workaround: There is no workaround.

- CSCse05777

  Symptoms: A router may reload unexpectedly when you configure more multilink interfaces than the maximum number that the router can support. The router should not reload but should generate an error message.

  Conditions: This symptom is observed on any Cisco router that imposes a limit on the number of multilink interfaces.

  Workaround: Do not exceed the maximum number of multilink interfaces.

- CSCse12198

  Symptoms: Individual B-channels on the primary T1 in the NFAS group sometimes go OOS for no reason.

Conditions: This symptom is observed when connected to a Cisco PGW that is running Cisco IOS Release 9.3(2). The Cisco AS5400 is connected to the Cisco PGW that is running RLM in the Signaling/Nailed mode.

Also, sometimes ISDN service goes OOS, and also channel states goes to 5 which is maintenance pending.

Workaround: When this happens, put ISDN service can be put back in service manually for individual CIC, but channel state cannot manually be put back in service unless the whole serial interface is bounced. This cannot be done when there is other traffic on the other b-channels.

- CSCse34162

  Symptoms: A Cisco router hangs after 5 to 10 minutes of passing traffic over a dialer interface.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 12.4(8) with PPP Multilink configured on a dialer interface and traffic is passing.

  Workaround: There is no workaround. A reboot is required to recover.

- CSCse78652

  Symptoms: The queuing mode on multilink interfaces erroneously defaults to fair-queuing instead of FIFO, causing distributed Cisco Express Forwarding (dCEF) to fail.

  Conditions: This symptom is observed on a Cisco 7500 series and occurs for all multilink interfaces. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse81069

  Symptoms: Unconfiguring the **isdn service b_channel** command is not taking effect. The command is not removed from the running configuration.

  Conditions: This symptom occurs when configuring the **isdn service b_channel** command to a state other than the default value of 0 on the ISDN D channel.

  Workaround: To remove the command, shut down the T1/E1 controller first and then unconfigure the command under the D channel serial interface.

- CSCsg15642

  Symptoms: A PSTN Gateway unexpectedly restarts due to a lack of memory. Overtime memory utilization increases, and the **show processes memory sorted** command indicates that the ISDN process is allocating an increased amount of memory.

  Conditions: This leak occurs when a SETUP message with Display IE is received.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg40885

  Symptoms: A router crashes during Online Insertion and Removal (OIR) on MLP- PPP on a Cisco 7200 platform.

  Conditions: This symptom is observed on a Cisco 7200 router that is configured for MLP-PPP.

  Workaround: Shut the multilink interface before doing an OIR.

- CSCsg50202

  Symptoms: When BRI interface flaps rapidly, ISDN Layer 1 detects link down, but Layers 2 and 3 keep active state during the transition. This may cause the BRI interface to get stuck, where subsequent incoming/outgoing call is rejected.

  Conditions: The symptom may be observed when cable is pulled out and put back rapidly.

  Workaround: Issue the **clear interface** command or the **shutdown** command followed by the **no shutdown** command on the affected BRI interface.

Resolved Caveats—Cisco IOS Release 12.4(8b)

Cisco IOS Release 12.4(8b) is a rebuild release for Cisco IOS Release 12.4(8). The caveats in this section are resolved in Cisco IOS Release 12.4(8b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCir00074

  Symptoms: A router crashes when the casnDisconnect object is set to “true” for a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series when you attempt to terminate the PPPoE session through SNMP by using the casnDisconnect object of the CISCO-AAA-SESSION-MIB.

  Workaround: There is no workaround.

- CSCsd26248

  Symptoms: A router set up to do dot1x authentication without accounting setup may experience a memory leak in process RADIUS until the process consumes all free memory.

  Conditions: This leak occurs on a router doing dot1x authentication without dot1x accounting configured and is sent attributes 24 (state) or 25 (class) from the Radius server.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCek14600

  Symptoms: A traceback has been seen on this release.

  Conditions: The symptom has been observed on Cisco IOS interim Release 12.4(04) T1fc2.

  Workaround: There is no workaround.

- CSCse29428

  Symptoms: A crash is seen with %ALIGN-1-FATAL after showing %SYS-2-CHUNKEXPANDFAIL and %SYS-2-MALLOCFAIL repeatedly.

  Conditions: This symptom is observed on a Cisco 3725 router that is running Cisco IOS Release 12.4(5a) with the c3725-advipservicesk9-mz image that is running IPSec VPN.

  Workaround: There is no workaround.

- CSCse56552

  Symptoms: Connections fail through a router that uses CBAC. The pre-gen session is created, and the download or transfer begins. The pre-gen session times out and gets deleted from the router. Since the full session never gets established, the connection then times out on the host.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(8) and using CBAC outbound on the outside interface when policy based routing is applied.

  Workaround: There is no workaround.

  Further Problem Description: This bug is first seen in Cisco IOS Interim Release 12.4(7.24).

- CSCse58419

  Symptoms: The memory consumption by the Chunk Manager process increases over time.

  Conditions: This behavior is observed on certain occasions when NAT is configured. When NVI with VRF is set in the system, the memory leaks rapidly. When NAT with VRF is set in the system, plus there is embedded address translation needed or skinny protocol traffic, the memory leaks in a slow pace.

  Workaround: There is no workaround.

- CSCse98590

  Symptoms: The router will display SYS-2-MALLOCFAIL messages on the console, and various protocols will operate erratically as a result of a low memory condition.

  Conditions: When a router has to duplicate incoming IPv4 multicast packets for transmission on multiple interfaces, and one of those interfaces is a GRE tunnel operating in GRE IPv6 mode, then memory used to duplicate that packet stream will not be freed. As a result, the router will soon exhaust all available memory.

  Workaround: The router will not exhaust memory if packets do not need to be duplicated (for example, if they enter on one interface and only exit the box through another interface), or if they do not need to duplicate to a tunnel interface that is running GRE over IPv6 (for example, tunnel mode GRE IPv4 does not have this problem).

- CSCsf27220

  Symptoms: A Cisco 7500 series router with any ATM Port Adapter may crash.

  Conditions: This symptom is observed when a router is configured with the Next Hop Resolution Protocol (NHRP) feature. When sending traffic, the router will crash.

  Workaround: There is no workaround.

ISO CLNS

- CSCse85158

  Symptoms: Locally advertised networks that are configured for the NSAP address- family under BGP will not be readvertised once they have been cleared from the BGP table.

Conditions: Once the **clear bgp nsap unicast *** command has been issued, the networks will no longer appear in the output of the **show bgp nsap unicast** command.

Workaround: There is no workaround.

Miscellaneous

- CSCej14709

  Symptoms: Minimal Disruptive Restart (MDR) does not function on a VIP4-50.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4.

  Workaround: There is no workaround.

  Further Problem Description: This caveat was opened to resolve an issue with enhanced Fast Software Upgrade (eFSU) for the Cisco 7500 series. However, the EFSU issue was resolved before EFSU was introduced in a hidden release for the Cisco 7500 series. (The EFSU feature is not generally available.)

- CSCek45461

  Symptoms: Path confirmation fails for voice calls on a Cisco AS5850. One-way audio may occur with manual phones.

  Conditions: These symptoms are observed on a Cisco AS5850 that processes MGCP, H.323, and SIP calls.

  Workaround: There is no workaround.

- CSCek52778

  Symptoms: Dialer idle timer is not reset by interesting traffic on ISDN NON- MLPP, Async MLPPP, Async PBR user sessions.

  Conditions: This symptom is found on a Cisco AS5850 that is running Cisco IOS Release 12.4(7b). Problem may occur with involvement of virtual profiles.

  Workaround: There is no workaround.

- CSCin99565

  Symptoms: A router that is configured for SSG may reload unexpectedly.

  Conditions: This symptom is observed when both the Transparent Auto-Logon (TAL) and Port-Bundle Host-Key (PBHK) SSG features are enabled and when it takes a long time before the AAA server responds.

  Workaround: There is no workaround.

- CSCsc97398

  Symptoms: The user information Layer 1 protocol may be included in the outgoing bearer capability and may be set to either G711 u-law or G711 A-law. Some PBXs may refuse the call because of this mismatch in the bearer capability.

  Conditions: This symptom is observed when a call is made from H.323 to ISDN with unrestricted digital information bearer capability.

  Workaround: There is no workaround.

- CSCsd37629

  Symptoms: Alignment errors and a bus error may occur on a Cisco platform that has the **ip inspect** command enabled.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: Disable the **ip inspect** command.

- CSCsd88768

  Symptoms: With PPP multilink configured on serial links on PA-MCX-8TE1,the following error message may be seen:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
  ```

  Conditions: With PPP multilink configured on serial links on PA-MCX-8TE1 and when traffic is flowing, the following error message may be seen:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
  ```

  Workaround: There is no workaround.

- CSCse05642

  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

- CSCse50887

  Symptoms: MGCP IOS Gateway sees the following:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  and then:

  ```
  config term router(UNKNOWN-MODE)
  ```

  Or, the **show running-config** command output is only 5 bytes.

  Conditions: This symptom occurs under the following conditions:

  – Use MGCP with the **ccm-manager config** command
  – Have more than 20 MGCP end points (voice ports)
  – Run Cisco IOS Release 12.3(11)T or later releases
  – Reset device pool from Cisco CallManager

  Workaround: Add the **no ccm-manager config** command.

- CSCse55652

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

Conditions: This symptom is observed on a distributed router such as a Cisco AS5850 or Cisco 7500 series that runs Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCse63494

  Symptoms: A router that is configured for Real-Time Protocol (RTP) may generate CPUHOG events and a traceback similar to the following:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (951/33),process = VOIP_RTCP.
  -Traceback= 0x60EA5A78 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  ```

  Alternatively, the router may unexpectedly reload and generate the following error message and traceback:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = VOIP_RTCP. -
  Traceback= 0x60EA5A58 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  %Software-forced reload
  Preparing to dump core...
  ```

  Conditions: This symptom is observed on a Cisco router that receives a badly formatted RTP Control Protocol (RTCP) packet.

  Workaround: There is no workaround.

  Further Problem Description: Typically, the badly formatted RTCP packet is produced by a device that does not conform to the RFC 3550 standard.

- CSCse64462

  Symptom: A Cisco Systems 7200 series router may encounter a block overrun with Redzone corruption, and subsequently crash if Turbo ACL is configured and the following command is entered:

  clear eou all

  Error messages similar to the following will be output, with associated tracebacks:

  ```
  %SYS-3-OVERRUN: Block overrun at <address> (red zone <value>)
  %SYS-6-BLKINFO: Corrupted redzone blk <address>
  ```

  Conditions: This symptom is observed on a Cisco 7200 series router running Cisco IOS Release 12.4 that is configured for Turbo ACL and when the following command is entered:

  clear eou all

  Workaround: Disable Turbo ACL by entering the following command:

  no access-list compiled

- 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

- CSCse68355

  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

- CSCse69335

  Symptoms: Media Gateway Control Protocol (MGCP) FXS/FXO port and Cisco IOS T1CAS resets during Hookflash transfer with CCM being the call agent.

  Conditions: This condition is seen when two consecutive RQNT messages with S: rel event is received at the Cisco IOS gateway. In this condition, the second RQNT message will not be acknowledged by the Cisco IOS gateway. This results in reset of all the MGCP endpoints on the Cisco IOS gateway.

  Workaround: There is no workaround.

- CSCse85329

  Symptoms: When you re-insert a PA-MC-8TE1+ port adapter in the same slot of a Cisco 7200 series via an OIR, the serial interface may enter the Down/Down state. When you enter the **shutdown** command followed by the **no shutdown** command on the T1 or E1 controller, the serial interface may transition to the Up/Down state, still preventing traffic from passing.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(7) or a later release.

  Workaround: Reload the router.

- CSCse89105

  Symptoms: RADIUS packets may be dropped or extra memory may be allocated when RADIUS packets are sent.

Conditions: These symptoms are observed on a Cisco platform that is configured for SSG when a RADIUS packet with a length of more than 1024 bytes is sent.

Workaround: There is no workaround.

- CSCse89402

  Symptoms: The CPU stack frame may become corrupted when a channel-group is configured on the T1/E1 controller.

  Conditions: This symptom is seen on mainboard WIC slots when the slot is configured for the “no network-clock participate.”

  Workaround: Use the VWIC in “network-clock participate” when installed in the mainboard WIC slot of the router.

  Further Problem Description: In most situations, no problems are seen. In rare cases, a crash may occur.

- CSCse93695

  Symptoms: Three-way calls that involve the Broadsoft SIP server and Cisco IAD2400 series Integrated Access Devices may not work.

  Conditions: This problem is observed in Cisco IOS Release 12.4(9)T.

  Workaround: There is no workaround.

- CSCse97112

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

  Conditions: This symptom is observed after the following command is issued:

  no x25 map compressedtcp a.d.c.d ip e.f.g.h [**options**]

  This may cause an Address Error (load or instruction fetch) exception, CPU signal 10.

  Workaround: There is no workaround.

- 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

- CSCsf09338

  Symptoms: The calls coming from the CMM MTP has one-way audio when a call transfer is done on the other side.

  Conditions: This symptom is observed when CMM is configured as MTP/XCode and running Cisco IOS Release 12.4(7b).

  Workaround: There is no workaround.

- CSCsf22493

  Symptoms: The Cisco Communication Media Module (CMM) crashes when processing the UnsubscribeDtmf message.

  Conditions: This symptom is observed when CMM XCODE/MTP is using Cisco IOS Release 12.4(8a) and RFC2833.

  Workaround: There is no workaround.

- CSCsg00602

  Symptoms: A Cisco 3845 or Cisco 3825 router with AIM-VPN/HPII-PLUS(EPII-PLUS) may show the following symptoms:

  1. show alignment errors
  2. crash by bus error
  3. XXX display by running the **show crypto engine accel ring packet** command
  4. if a telnet session, which shows symptom three, is cut by "clear line," its related exec process does not disappear and starts to occupy CPU.

  Conditions: This failure is seen on the Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco 1800 series routers that are configured with an AIM-VPNII or AIM-VPNII PLUS Virtual Private Network (VPN) encryption and hardware advanced integration module (AIM).

  Workaround: Avoid running the **show crypto engine accel ring packet** command.

Wide-Area Networking

- CSCek28604

  Symptoms: A Cisco device may reload ("System returned to ROM") unexpectedly due to a memory leak in the ISDN L2 process.

  Conditions: This symptom is observed on a Cisco device that functions in a call manager-backhaul configuration after running under stress for about 24 hours.

  The output of the **show processes memory**, collected in regular intervals shows a memory leak in the ISDN L2 process. The amount of memory that is held by the ISDN L2 process will be very large and growing.

  Workaround: Enter the **isdn k 1** command on all backhauled serial interfaces.

- CSCek55209

  Symptoms: If the **ppp multilink endpoint mac** *interface* command or the **ppp multilink endpoint ip** *a.b.c.d* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual-circuit is unconfigured.

  Conditions: This symptom is observed on a router with Multilink PPP.

  Workaround: Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCse79994

  Symptoms: BRI Layer 2 remains in the ESTABLISH_AWAITING_TEI state instead of entering the MULTIPLE_FRAME_ESTABLISHED state.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf03251

  Symptoms: Primary and backup NFAS interfaces may transition from WAIT to OOS even after receiving “in-service” message from the PSTN.

  Conditions: This symptom is observed on a Cisco AS5400XM that is running several Cisco IOS 12.4 mainline and 12.4T releases.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(8a)

Cisco IOS Release 12.4(8a) is a rebuild release for Cisco IOS Release 12.4(8). The caveats in this section are resolved in Cisco IOS Release 12.4(8a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek33076

  Symptoms: A RADIUS progress code is incorrectly reported for a call that fails at IPCP. The progress code reports that the Link Control Protocol (LCP) is the open state.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(3a) and that is configured for AAA.

  Workaround: There is no workaround.

- CSCin99788

  Symptoms: %AAA-3-ACCT_LOW_MEM_TRASH error message spewed when run into low memory, and AAA related data could be leaked after hitting this condition.

  Conditions: The likely trigger is an interface flap with a huge number of sessions going down simultaneously generating enormous accounting-stop records. A sluggish/unreachable AAA server IO memory would be held for a long time retrying to send the accounting records.

  Workaround: There is no workaround.

- CSCsc97727

  Symptoms: An access point may crash when you add or remove TACACS servers via the CLI.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(7)JA1 or Release 12.3(7)JA2 and that has the **aaa accounting commands** *level* **default** *list-name* **group** *groupname command enabled. The symptom may also occur in other releases.*

Workaround: Disable the **aaa accounting commands** *level* **default** *list-name* **group** *groupname command.*

Alternate Workaround: Use RADIUS instead of TACACS.

- CSCsd99763

  Symptoms: A Cisco 7200 series router reloads unexpectedly while configuring BGP access list.

  Conditions: This symptom is observed on a Cisco 7206VXR (NPE-G1) processor (revision A). The following commands serve as an example that causes router to reload unexpectedly:

```
config t
router bgp 100
neighbor EXTERNAL route-map MAP3 out
address-family ipv4 multicast
neighbor EXTERNAL route-map MAP3 out
!
ip as-path access-list 1 deny ^$
ip as-path access-list 2 permit ^(700)+(_1123)|_2374$|^(_700)+(_2374)+
(_1123)+$
ip as-path access-list 3 permit _3400_
ip as-path access-list 4 permit ^(700)+(_3400)|_1123$|^700$|_23\[0-9\]$
!
route-map MAP3 permit 10
match as-path 1
!
route-map MAP3 deny 20
match as-path 2
!
route-map MAP3 permit 30
match as-path 3
!
route-map MAP3 permit 40
match as-path 4
set metric 300
end
```

  Workaround: There is no workaround.

- CSCse49728

  Symptoms: SNMPv3 informs are not sent out after a device reload.

  Conditions: This symptom is observed when SNMPv3 informs have been configured, and the device is reloaded.

  Workaround: Re-enter any of the **snmp-server host** commands.

Interfaces and Bridging

- CSCek27833

  Symptoms: Pings with a datagram size of 1485 and above are not going across the bridge.

  Conditions: This symptom is observed on a serial interface configured for PPP and part of the bridge group on a Cisco router.

  Workaround: Increase the MTU size on the interfaces. For example, configure an MTU of 1524.

IP Routing Protocols

- CSCed84633

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

  Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206. 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 fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCek29860

  Symptoms: A Cisco router may experience a software-forced crash.

  Conditions: This symptom is observed on a Cisco router that is configured for secure NAT (SNAT), NAT Stateful Failover, and HSRP.

  Workaround: There is no workaround.

- CSCek42134

  Symptoms: NAT Virtual Interface (NVI) per VPN routing/forwarding (VRF) is broken from inside to outside. The router shows CEF drops for the destination prefix existing for a route for this prefix on VRF table.

  Conditions: This symptom has been observed on Cisco IOS Release 12.3(14)T6 and Interim Release 12.4(7.20)T.

  Workaround: Configure static translation for the destination prefix to itself.

- CSCek43945

  Symptoms: A memory leak may occur on a router that is configured for NAT and the router may eventually run out of memory.

  Conditions: This symptom is observed on a Cisco router when NAT is configured.

  Workaround: There is no workaround.

- CSCse04037

  Symptoms: A ping or a Telnet connection from an inside gateway to an outside gateway through a router that is configured for NAT may fail because of an error in the NAT table lookup process.

Conditions: This symptom is observed on a Cisco router when the **preserve-port** keyword is not configured in the **ip nat service** command and occurs whether or not NAT Overload is configured.

Workaround: There is no workaround.

- CSCse04220

  Symptoms: The BGP table version remains stuck at 1 following the issue of the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6.

  Issuing the **clear bgp ipv4 uni *** or **clear bgp ipv6 uni *** commands may also result in a crash.

  Conditions: This symptom occurs when issuing the **clear bgp ipv4 uni *** or **clear bgp ipv6 uni *** commands.

  Workaround: Using the **clear ip bgp *** command clears the sessions, and the BGP table is purged. The **clear ip bgp *** command will also avoid crashing the router.

ISO CLNS

- CSCuk60585

  Symptoms: A router that is configured for redistribution into ISO-IGRP may crash.

  Conditions: This symptom is observed when the configuration is nvgened.

  Workaround: There is no workaround.

Miscellaneous

- CSCeg03885

  This caveat consists of two symptoms, two conditions, and two workarounds, and only refers to routers that are configured with MPLS TE tunnels:

  Symptom 1: Momentary packet loss may occur during tunnel reoptimization, usually several times between the creation of a new tunnel and the cleanup of the old tunnel. Sometimes, longer packet loss may occur during tunnel reoptimization.

  Condition 1: This symptom is observed on any MPLS TE tunnel when the reoptimized label switched path (LSP) traverses a midpoint or headend router that runs Cisco IOS Release 12.0(25)S4.

  Workaround 1: There is no workaround.

  Symptom 2: Permanent bad labels may be present after MPLS TE tunnel reoptimization.

  Condition 2: This symptom is observed on a router that runs a Cisco IOS image that does not include the fix for CSCed21063 and that functions in a network in which some routers run Cisco IOS Release 12.0(25)S4. With the exception of Release 12.0(25)S4 itself, Cisco IOS software releases that are listed in the “First Fixed-in Version” field at the following location are not affected: http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed21063.

  Workaround 2: There is no workaround. To recover from the symptoms, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected TE tunnel interface.

- CSCei84353

  Symptoms: A router crashes when you remove an Embedded Event Manager (EEM) applet.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S but is not platform- and release-dependent. This symptom occurs under the rare occasion that the EEM applet is removed while EEM is attempting to trigger the applet for execution.

Workaround: Perform the following three steps:

1. Before you remove the EEM applet, disable EEM applet scheduling by entering the **event manager scheduler applet suspend** command.
2. Remove the applet.
3. After you have removed the applet, re-enable EEM applet scheduling by entering the **no event manager scheduler applet suspend** command.

- CSCej29710

  Symptoms: Unable to send EEM type system SNMP trap notifications.

  Conditions: This symptom occurs when users want to send EEM SNMP system type trap notifications upon triggering of a policy.

  Workaround: In EEM applet mode if a user desires an SNMP notification upon event trigger, they should specify it as an action by using the **action snmp-trap** command. In EEM TCL policies, use the **action_snmp_trap** TCL command.

- CSCek26155

  Symptoms: A recursive pattern scan loop can occur when the Embedded Event Manager (EEM) CLI ED attempts to scan for patterns provided by action CLI commands.

  Conditions: This issue occurs when an applet contains a CLI event that is scanning for a pattern that is given as a CLI command in one of its actions. See the following example:

```
event manager applet one
   event cli pattern "show version" sync yes
   action 1 cli command "show version"
```

  In this example the action being performed causes the event to trigger in a loop.

  Workaround: Do not use an action CLI command containing a pattern that matches the CLI event pattern.

- CSCek42816

  Symptoms: A voice gateway reloads while bulk calls are being processed.

  Conditions: The symptom is observed on a Cisco voice gateway that runs VXML applications that stream voice when the voice gateway receives prompts from an HTTP server.

  Workaround: Enter the **ivr prompt streamed none** command on the voice gateway.

- CSCek43642

  Symptoms: When you try to remove an Embedded Event Manager (EEM) policy that has event criteria specified via the **event_register_appl** Tcl command extension, the attempt fails.

  Conditions: This symptom is observed when two or more Embedded Event Manager policies are configured and when only one of these policies has event criteria specified via the **event_register_appl** Tcl command extension.

  Workaround: There is no workaround.

- CSCek47283

  Symptoms: A router cannot be reloaded by entering the **reload** command, and the following message is displayed when you attempt to reload the router:

  The startup configuration is currently being updated. Try again.

  Conditions: This symptom is observed under rare conditions and may be triggered after an "Invalid pointer value in private configuration structure" error message is displayed (as seen in caveat CSCin98933). This symptom is observed in Cisco IOS interim Release 12.3(19.7), interim Release 12.4(6.5), and interim Release 12.4(6.5)T, and in later releases.

  Workaround: There is no workaround.

- CSCsb95563

  Symptoms: On rare occasions, Embedded Event Manager (EEM) may cause a crash when you deregister an EEM policy.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series but is platform-independent.

  Workaround: There is no workaround.

- CSCsb99936

  Symptoms: The **show ephone** command reveals a call is stuck in the SEIZE state instead of progressing to the correct state during a call.

  Conditions: This symptom has been observed when an H.323 call is placed from CME to a non-CME H.323 endpoint.

  Workaround: There is no workaround.

- CSCsc18707

  Symptoms: No error message is printed out when running an Embedded Event Manager (EEM) policy that is not registered with the none event detector.

  Conditions: This symptom occurs when executing **event manager run** *policy name* or **action label policy** *policy name* command, but the policy is not registered with the none event detector.

  Workaround: There is no workaround.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that is running Cisco IOS Release 12.4(3)B. The router has services 81, 82 and 90 configured. The only service having a problem is 90. The packet traces indicate that the router is sometimes responding to Here_I_Am messages from the cache with I_See_You messages containing an incorrect destination IP address. This leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(3)B.

  Workaround: There is no workaround.

- CSCsd34114

  Symptoms: A router that is running Cisco IOS with an IPv6 localpools configuration may reload under rare circumstances.

  Conditions: The IPv6 localpool has to allocate prefixes to the same username on multiple interfaces in a specific order, then release one of the prefixes, and try to allocate a new prefix.

  The interfaces that the prefixes are allocated on, and the ordering of the events, need to follow a very specific pattern in order to create the issue.

Workaround: Use Per-User prefixes from a RADIUS server, or in DHCP-PD, use the prefix allocation per DUID.

Further Information: IPv6 localpools are currently used by IPv6CP (IPv6 over PPP links) and DHCP-PD.

This problem is unlikely to be observed with IPv6CP.

- CSCsd66800

  Symptoms: MGCP Gateway Controlled T38 fax-relay call is getting disconnected.

  Conditions: This symptom has been observed while making a Gateway-controlled fax call using MGCP.

  Workaround: There is no work around.

- CSCsd73526

  Symptoms: When using CSS in a design for CVP, the Cisco IOS Voice Browser cannot play the media file after upgrading the Cisco IOS from Cisco IOS Release 12.3(3a) to Release 12.4(3b). CSS does send the HTTP Redirect pointing to CVP, but the gateway does nothing with it.

  Conditions: This symptom has been observed when the following are present:

  - AS5400HPX
  - Cisco IOS Release 12.4(3b)
  - CVP 3.1 SR1
  - ICM 6.0
  - CallManager 4.1(3) SR 2

  Workaround: Bypass CSS, and point the VXML application directly to CVP.

- CSCsd76444

  Symptoms: There is an unexpected reload of a Cisco router that is running PRE experiencing Signal 0 reload with no stack contents.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running PRE.

  Workaround: There is no workaround.

- CSCse01124

  Symptoms: The Hot Standby Router Protocol (HSRP) may not come up and may remain in the “Init” state, which can be verified in the output of the **show standby brief** command.

  Conditions: This symptom is observed when dampening is configured on a native Gigabit Ethernet interface of a Cisco 7200 series or on a Fast Ethernet interface of a PA-FE-TX port adapter. Other types of interfaces are not affected.

  Workaround: When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Gigabit Ethernet and Fast Ethernet interfaces of all routers of the standby group.

  To prevent the symptom from occurring, remove dampening from the Gigabit Ethernet and Fast Ethernet interfaces.

- CSCse15025

  Symptoms: An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

When this problem occurs, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

Because this issue impacts the signaling channels, it has been seen that calls either will not connect at all through impacted ports or in some cases when multiple simultaneous calls are present on adjacent voice ports/timeslots, the call may connect momentarily before being disconnected.

If a problem occurs only on a single voice port, there is another problem, not this caveat (CSCse15025). PRI/BRI calls are not affected because PRI/BRI does not utilize the DSP for signaling purposes.

When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port- number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41, and 42 is presented and some of the registers show double- octet information. See the example output (2) below.

When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** *port- number* **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

Further Problem Description: The changes in CSCse15025 includes changes in CSCsc11833 and CScsd90851. These changes have been shown to help mitigate this problem in the majority of cases.

There is a further detection and reset mechanism in CSCse15025 that will recover the DSP which is in this state. This mechanism will trigger immediately if the impacted voice port is an analog FXO port. For other voice ports, a delay in the detection will be present and it is possible to see the symptom of this problem before the recovery code triggers.

Note that the reset mechanism will cause any active calls utilizing the DSP in question to be dropped.

It is recommended if running with modules which can be impacted by this issue to upgrade to a release of software which contains the changes in CSCse15025. If the DSP is reset and the below output is seen, contact the TAC for further assistance. Note that this output is sent at debug level and it is recommended to enable either syslog or logging buffered on the gateway.

Logging buffered on the gateway is enabled through the global command **logging buffered 50000 debug** as an example to set the logging buffered to use 50K bytes of processor memory for logging. The output of the log can be seen with the exec command **show log**.

Example output when detection and recovery code on gateway triggers:

```
*May 31 14:30:43.343: TDM pointers: 0100 0100 0115 0115. Deltas: 0001 0000.

*May 31 14:30:43.347: Received alarm indication from dsp(0/1)
0030 0000 0080 0000 0013 4100 2E2E 2F2E 2E2F 6D6F 6475 6C65 732F 7363 6865
6475 6C65 2F64 6562 7567 2E63 2833 3634 2900
*May 31 14:30:43.347: ../../modules/schedule/debug.c(364)

*May 31 14:30:43.347: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to Administrative Shutdown
*May 31 14:30:43.647: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
```

```
changed state to Administrative Shutdown
*May 31 14:30:43.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to Administrative Shutdown
*May 31 14:30:44.247: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to Administrative Shutdown

*May 31 14:30:48.147: Crash dump CLI may not be configured, not able to get
crash info, slot 0, dsp 1
*May 31 14:30:48.147: DSPDUMP - Recover slot 0 dsp 1
*May 31 14:30:48.147: DSPDUMP - ka sent 0, ka_cnt 51193, skip_ka 103079
*May 31 14:30:50.579: %DSPRM-5-UPDOWN: DSP 1 in slot 0, changed state to up
*May 31 14:30:50.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to up
*May 31 14:30:51.219: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to up
*May 31 14:30:51.371: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to up
*May 31 14:30:51.523: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to up
```

Following are command output examples:

1) Following is an example of normal output for FXO and EVM FXS ports.

For FXO ports, the value is usually 0x01 but for EVM FXS the value can be different. When you run the above-mentioned command, the expected output is that a single octet is displayed and only for register 39. (This command does not work for VIC-4FXS and VIC2-xFXS modules).

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x01
```

2) Following is an example of output for FXO and EVM FXS ports that indicates that the symptom has occurred. Note that the exact output for the register values is different, but when the symptom occurs, different lines with information are displayed as shown below:

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF
```

3) Following is an example of normal output for FXS and analog E&M modules. The values that are listed in a normal case may be different, but only four registers of a single octet should be displayed.

```
Values read from PEB2465 Codec connected to DSP 02 (channel 0):
------------------------------------------------------------
```

```
Extended Register Values (XR4..XR1) = 00, CC, 50, 11
```

4) Following is an example of output for FXS and analog E&M modules that indicates that the symptom has occurred.

```
Values read from PEB2x65 Codec connected to DSP 0, channel 1:
------------------------------------------------------------

Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCse16494

  Symptoms: Traffic does not flow after a Route Processor Redundancy Plus (RPR+) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 and that is configured for RPR+.

  Workaround: After the RPR+ switchover has occurred, reload microcode onto the router.

- CSCse34097

  Symptoms: When a voice call is made to one of the busy channels of BRI/PRI port, the call gets rejected and then another call is made to the available port. The call gets connected, and the user hears an annoying hissing sound.

  Conditions: The procedure to recreate this scenario is the following:

```
Phone a & b ---OGW --VoIP --TGW(2611) --BRI/PRI --PBX -- phone c & d


Phone a calls phone c;
Phone b calls phone c;
Phone b calls phone d;


Phone d picks up and hears a hissing noise.
```

  Workaround: There is no workaround.

- CSCse39452

  Symptoms: OGW rejects incoming OLC from an alternate endpoint when the slow start procedure is used and so the call is rejected.

  Conditions: This symptom has been observed when OGW is configured to use the slow start procedure.

  Workaround: There is no workaround.

  Further Problem Description: OGW is configured to use the slow start procedure. OGW receives alternate endpoints in the ACF. The call on the primary endpoint fails after H.245 procedures are completed and logical channel are opened. Now OGW tries the call on alternate endpoint, but it rejects the incoming OLC from the alternate endpoint, thus resulting in call failure.

- CSCse45425

  Symptoms: VAM2 resets with the message “Free Pool stuck”. The IPSec SAs are transferred to software crypto. This causes 100% CPU.

  Conditions: The decrypted packet total size does not match the total length in its IP header.

  Workaround: There is no workaround for the VAM2 reset. However, during the VAM2 recovery, disable software encryption by issuing the **no crypto engine software ipsec** command to force encryption back to hardware.

- CSCse49985

  Symptoms: A Cisco 3745 router crashes due to a software-forced crash. An error message similar to the following is displayed:

  ```
  rcojx67-vgw01-3745 uptime is 1 day, 16 hours, 19 minutes
  System returned to ROM by error - a Software forced crash, PC 0x60A87D38
  at 15:59:36 GMT Tue May 16 2006
  System restarted at 16:00:35 GMT Tue May 16 2006
  System image file is "flash:c3745-ipvoice-mz.123-14.T3.bin"
  ```

  Conditions: This symptom has been observed with a Cisco 3745 router running Cisco IOS Release 12.3(14)T3. This symptom is also seen when there are some memory allocation failures.

  Workaround: There is no workaround.

- CSCse56660

  Symptoms: Inbound calls to FXO ports on Cisco IOS VoIP gateways connect, but audio is not present.

  Conditions: With **caller-id enable** configured on FXO ports, the call will connect, but no audio is heard. When this occurs, the following error message can be seen at debug level:

  ```
  Jun 20 01:41:15.855: mbrd_e1t1_vic_connect: setup failed
  Jun 20 01:41:15.855: flex_dsprm_tdm_xconn: voice-port(0/0/1), dsp_channel
  (/0/2/0)
  ```

  Workaround: Disable caller id on the voice-port.

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

  Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third party system.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek40618

  Symptoms: A router may crash by address error (load or instruction fetch) exception during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCsd19867

  Symptoms: BRI interfaces does not come up when you reload a router. You must enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected BRI interfaces to bring them up.

  Conditions: This symptom is observed when you enter the **no isdn spoofing** command and reload the router.

  Workaround: Disable the **no isdn spoofing** command.

- CSCsd81350

  Symptoms: When asynchronous serial interfaces are used as member links in multilink PPP bundles, the router may crash due to memory corruption.

  Conditions: This problem can occur under conditions where multilink fragmentation is done, and where the bundle includes at least one member link that is an asynchronous interface.

  Workaround: Disable fragmentation on the bundle interface for any bundle that may include asynchronous links as members. Alternatively, if the use of multilink is not a requirement, disable multilink on the asynchronous interfaces.

- CSCse16539

  Symptoms: VPDN loadbalancing incorrectly biases to one LNS (IP address) instead of sharing the session load between the different LNSs after LNS return from the busy list.

  Conditions: This occurs when multiple LNSs are configured for one vpdn-group and are unreachable. They are moved to the busy list. Once the LNSs become reachable again, this problem occurs.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(8)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(8). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(8). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCea36491

  Symptoms: When a Telnet session is made to a router after a VTY session pauses indefinitely, the user in the Telnet session may not be able to enter the configuration mode. When these symptoms occur, interfaces may enter the wedged state with Simple Network Management Protocol (SNMP) traffic.

  Conditions: This behavior is observed on ATM and Packet over SONET (POS) interfaces. This behavior is not platform-specific.

  Workaround: Disable Simple Network Management Protocol (SNMP) configuration traps by entering the **no snmp-server enable traps** config global configuration command.

- CSCee41892

  Symptoms: A VIP4-80 card may fail to load the Cisco IOS software image. When this situation occurs, the following error messages are generated:

  ```
  %DBUS-3-SW_NOTRDY: DBUS software not ready after HARD_RESET, elapsed 13056, status 0x0
  %DBUS-3-WCSLDERR: Slot 2, error loading WCS, status 0x4 cmd/data 0xDEAD pos 97
  %DBUS-3-WCSLDERR: Slot 2, error loading WCS, status 0x4 cmd/data 0xDEAD pos 99
  %UCODE-3-LDFAIL: Unable to download ucode from system image in slot 2, trying rom ucode
  %RSP-3-NOSTART: No microcode for VIP4-80 RM7000 card, slot 2
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when you enter the **microcode reload** command.

Workaround: There is no workaround.

Further Problem Description: The symptom may also occur because of improperly installed line cards. If this situation occurs, re-install the line cards.

- 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.

- CSCeg24855

  Symptoms: A platform reloads after you enter the **aaa route download 2** command.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.3(11)T2.

  Workaround: There is no workaround.

- CSCej30903

  Symptoms: A router allows logging into the root (or any other configured) view without prompting for a password.

  Conditions: This symptom is observed when no method list is configured for login service.

  Workaround: Configure a method list for the login service.

- CSCek27271

  Symptoms: The IPSLA test packets returned by the IPSLA responder for the UDP jitter operation have ToS value of 0 instead of the value configured for the operation. Because of this, the two IPSLA UDP jitter operations between same source and responder routers with just the different ToS configurations will report the same round trip time even though the expected values are different.

  Conditions: This symptom has been observed on the routers configured with an IP SLA User Datagram Protocol (UDP) jitter operation with microseconds precision and has the ToS value configured.

  Workaround: There is no workaround.

- CSCek32365

  Symptoms: A Cisco 7500 series that is configured with more than two VIP 4-80 or VIP 6-80 processors may crash during the boot process and may not boot at all.

  Conditions: This symptom is observed on a Cisco 7500 series that runs a Cisco IOS software image that includes he fix for caveat CSCei45236. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCei45236. 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.

- CSCek36902

  Symptoms: A Cisco 7500 series may generate a “%CBUS-3-CMDONPROC” error message and a traceback.

  Conditions: This symptom is observed on a Cisco 7500 series with a Fast Serial Interface Processor (FSIP) when you perform an OIR.

  Workaround: There is no workaround.

- CSCek40060

  Symptoms: RADIUS server authentication may not function for dialup and PPP clients.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) and that has the **radius-server retry method round-robin** command enabled.

  Workaround: Disable the **radius-server retry method round-robin** command. Note that the symptom does not occur in Release 12.3 or Release 12.3T.

- CSCsb30875

  Symptoms: Active eRSC on a Cisco AS5850 gateway could hang after RPR+ failover, if the **aaa accounting system** command is configured.

  Conditions: The symptom has been observed under the following conditions:

  1. RPR+ failover occurred.
  2. Console connection window closed & reopened to the newly active eRSC after failover.

  Workaround: There are two workarounds.

  1. The eRSC hang will not happen if no attempt is made to close and reopen the console session with newly active eRSC after failover.
  2. Remove the **aaa accounting system** command from the configuration.

- CSCsb43767

  Symptoms: RADIUS stop packets that are sent to a RADIUS server may contain an incorrect value for the NAS-Port attribute (RADIUS IETF attribute 5). Information that is related to the asynchronous interface is not included in the Cisco-NAS-port VSA.

  Conditions: This symptom is observed on when a Cisco router sends stop packets to a RADIUS server via an asynchronous interface.

  Workaround: There is no workaround.

- CSCsb71584

  Symptoms: A spurious memory access is generated in the “aaa_string_vsa_prefix_to_protocol” function.

  Conditions: This symptom is observed on a Cisco platform that is configured for Network Admission Control (NAC).

  Workaround: There is no workaround.

- CSCsc19289

  Symptoms: MC-T1 is disabled and wedged when changing the MTU size on the MC-T1 interface.

  Conditions: This symptom has been observed when dLFIoLL is configured on a Cisco 7500 router and the MTU size on MX-serial interface is changed.

  Workaround: Remove and replace the MC-T1 or micro reload the MC-T1.

- CSCsc27380

  Symptoms: On the console of the active RSP of a Cisco 7500 series, “IPC_RSP_CBUS-3-NOHWQ” error messages are generated.

  Conditions: This symptom is observed on a Cisco 7500 series that functions in SSO mode when you remove the standby RSP via a soft OIR.

  Workaround: There is no workaround.

- CSCsc70055

  Symptoms: A Cisco 7200 series may crash when you perform a graceful OIR of a port adapter that is processing traffic.

  Conditions: This symptom is observed mostly when the port adapter processes ingress traffic.

  Workaround: Do not perform a graceful OIR. Rather, perform a manual OIR.

- CSCsd10306

  Symptoms: IP SLA packets are dropped in the network. They may also cause a buffer leak on some Cisco routers. Frequency of the problem is very low, less then 1%.

  Conditions: This symptom is observed on IP SLA packets that have an MPLS label applied on the source router.

  Workaround: There is no workaround.

  Further Problem Description: The IP SLA packets in question have a corrupted IP header.

- CSCsd20739

  Symptoms: A router that has a GRE IPSec tunnel may hang and all routing neighbors may be dropped.

  Conditions: This symptom is observed when the GRE IPSec tunnel is configured for PIM sparse mode and OSPF, when traffic levels are moderate, and when you enter the **ip flow egress** command on a tunnel interface.

  Workaround: Do not enter the **ip flow egress** command on a tunnel interface. When the symptom has occurred, disable NetFlow Export to restore proper router operation.

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

  Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

  Workaround: There is no workaround.

- CSCsd26831

  Symptoms: When you enter the **show snmp mib ifmib ifindex**, the router generates an "% Incomplete command" error message because the carriage return option is not present.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(7.4).

  Workaround: There is no workaround.

- CSCsd63874

  A traceback may occur in the "send_link_monitor_config_cmd" function and the following error message may be generated:

  ```
  %CBUS-3-CMDONPROC: Cmd not interrupt protected
  ```

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

  Workaround: There is no workaround.

- CSCsd63890

  Symptoms: A traceback is generated on a Cisco platform that has NetFlow configured on an interface.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 or Release 12.4T when you enter the **ip route-cache flow** or **ip flow ingress** command on an interface.

Workaround: Do not configure NetFlow on an interface.

- CSCsd65404

  Symptoms: Control packets are not properly marked with the ToS setting that is specified in an IP SLA probe. Only the data packets are marked with the configured ToS setting.

  Conditions: This symptom is observed when an IP SLA probe is configured via SNMP. Note that the symptom does not occur when the IP SLA probe is configured via the CLI.

  Workaround: Configure the IP SLA probe via the CLI. However, this workaround does not scale well for networks in which a large number of probes must be configured.

EXEC and Configuration Parser

- CSCsd32923

  Symptoms: A router may unexpectedly reload with a bus error when you enter a command while the command buffer is full of white space.

  Conditions: This symptom is observed when you enter a partial command and when the tab key is used while the command buffer is full.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCdp08975

  Symptoms: Even though traffic is flowing through ATM VCs, the status of the ATM VCs may change unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series that has RFC1577 configured on the main interface and that does not function as an Address Resolution Protocol (ARP) server.

  Workaround: Do not configure RFC1577 on the main interface. Rather, configure RFC1577 on a subinterface.

- CSCek27126

  Symptoms: A router may crash when you remove a label-controlled ATM (LC-ATM) subinterface and may generate an "%ALIGN-1-FATAL: Corrupted program counter" error message.

  Conditions: This symptom is observed on a Cisco 7200 series but may be platform-independent.

  Workaround: Shut down the main interface before you remove the subinterface.

- CSCsc66187

  Symptoms: Error messages such as the following one may be generated on a Cisco 7500 series or Cisco 7600 series:

  ```
  %CWPA-3-IPCALLOCFAIL: Failed to allocate IPC buffer for loveletter data
  ```

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured with a 1-port Packet-over-SONNET OC-3c/STM-1 multimode port adapter (PA-POS-OC3MM) when you enter the **no shutdown** interface configuration command on the interface.

Workaround: There is no workaround.

- CSCsd41989

  Symptoms: A T3 controller remains down when loopback local is configured.

  Conditions: This symptom is observed on a Cisco platform that is configured with a channelized T3 port adapter when the T3 controller is in an unavailable seconds (UAS) state.

  Workaround: Remove the cause of the UAS state for the T3 controller.

- CSCsd49253

  Symptoms: A Cisco 7200 series may reload unexpectedly when an Automatic Protection Switching (APS) switchover occurs on Packet over SONET (POS) interfaces that are configured for redundancy.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCsd63918

  Symptoms: A router reloads unexpectedly when you enter the **bridge-group** *bridge-group* command as part of an ATM PVC configuration.

  Conditions: This symptom is observed on a Cisco router that is configured with an ATM port adapter such as a PA-A2 port adapter.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeg39601

  Symptoms: The IPv6 multicast RP encapsulation tunnel remains down.

  Conditions: This symptom occurs on the configuration of the **ipv6 pim rp-address** command. The resulting encapsulation tunnel is created but remains always in down state.

  Workaround: There is no workaround.

- CSCej78303

  Symptoms: A router may crash when you disable the **ipv6 multicast-routing** command.

  Conditions: This symptom is observed when you enable and disable the **ipv6 multicast-routing** command multiple times while IPv6 Multicast traffic is being processed.

  Workaround: There is no workaround.

- CSCek25582

  Symptoms: Spurious memory accesses may be (continuously) generated at the “igmp_process_timers” function.

  Conditions: This symptom is observed on a Cisco router that is configured for multicast routing.

  Workaround: There is no workaround.

- CSCek32244

  Symptoms: Not all classful networks are locally generated in the BGP table.

  Conditions: This symptom is observed on a Cisco router that has the **auto-summary** command enabled and occurs when classful networks are provided before the routes are made available in the routing table.

Workaround: There is no workaround.

- CSCek33991

  Symptoms: A router may reset unexpectedly when it is in the midst of output of the results of the **show interface dampening** command, and the interface is deleted from another vty connection.

  Conditions: This symptom can be encountered if concurrent connections are opened to a router, and the **show interface dampening** command is issued while interface(s) are deleted.

  Workaround: Ensure interfaces with **dampening** configured are not deleted while the **show interface dampening** command can be possibly issued on another vty.

- CSCsa87034

  Symptoms: When you attempt to clear the routing table, the neighbor is brought down instead.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 unicast *** or **clear bgp ipv6 unicast *** command, causing respectively the IPv4 neighbor or IPv6 neighbor to be brought down.

  Workaround: There is no workaround.

- CSCsc00378

  Symptoms: Changes in an export map are not picked up by the BGP Scanner.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when you apply an export map to a VRF and when the interface that connects the PE router to a CE router is configured for OSPF.

  Workaround: Enter the **clear ip ospf process** command to enable the BGP Scanner to pick up the changes in the export map.

- CSCsc19256

  Symptoms: When NAT overload is configured on a PE router, a traceroute from a VRF client to a gateway fails when the PE router is indirectly connected to the gateway via a VPN interface or generic interface.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has NAT overload configured.

  Workaround: There is no workaround.

- CSCsc46337

  Symptoms: When about thousand eBGP connections are opened between two routers that are connected back-to-back, additional point-to-point eBGP connections between the routers are not established even if IP connectivity between the BGP next-hops is provided.

  Conditions: This symptom is observed when one Cisco router functions as a PE router and the other Cisco router functions as a CE router that has VRF-lite configured.

  Workaround: Reload the PE router to enable all sessions to become established, including the ones that previously were not established.

- CSCsc56595

  Symptoms: When an OSPFv3 router has more IPv6 prefixes in a single OSPFv3 area than can be advertised in a single intra-area prefix Link State Advertisement (LSA) that is small enough to be advertised via the normal IPv6 Maximum Transmission Unit (MTU), the additional IPv6 prefixes are not advertised.

Conditions: This symptom is observed when many interfaces with IPv6 global addresses are configured in a single OSPFv3 area and when the size of the LSA is less than the normal IPv6 interface MTU.

Workaround: Spread the IPv6 interfaces over multiple OSPFv3 areas.

- CSCsc62333

  Symptoms: Application Layer Gateway (ALG) traffic does not traverse a router that is configured for NAT and that has a NAT Virtual Interface (NVI)

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4 or Release 12.4T. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsc72090

  Symptoms: A router that is configured for EIGRP may fragment packets if the MTU on the interface is set to a value that is lower than 1500 bytes. This situation may cause additional overhead for the receiving router that must reassemble the packets.

  Conditions: This symptom is observed on a Cisco router that transmits packets that are larger than the MTU on the interface and occurs because EIGRP does not automatically adjust to the value of the MTU on the interface.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat prevents EIGRP from sending packets that are larger than the MTU of the interface MTU in order to prevent fragmentation.

- CSCsc76327

  Symptoms: When a VRF route is redistributed into the MP-BGP cloud, a routing loop may occur for the prefix (that represents the VRF route) between the EIGRP cloud and the MP-BGP cloud.

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

  – The router has EIGRP configured on the link to a CE router.

  – The router has a static VRF route that is redistributed into the configuration that is defined by the **address-family vrf** *vrf-name* command and that is part of the BGP routing process.

  Workaround: There is no workaround. Applying a route map with a pre-bestpath option does not resolve the loop.

- CSCsc78813

  Symptoms: While using NAT in an overlapping network configuration, the IP address inside a DNS reply payload from the nameserver is not translated at the NAT router.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(18) and that has the **ip nat outside source** command enabled. The symptom could also occur in Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsc94867

  Symptoms: A traceback is generated in the log after NAT entries are created on a PE router that is configured for NAT and that has a static NVI.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(5.12) or interim Release 12.4(5.13)T2.

  Workaround: There is no workaround.

- CSCsc98828

  Symptoms: PIM becomes disabled on an output interface, preventing packets from being sent, and causing the SR flag to be set after 60 seconds on the router that functions as the first hop.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 PIM.

  Workaround: There is no workaround.

- CSCsd01824

  Symptoms: Extended NAT entries that are created by outside static NAT translation in a VRF SNAT environment do not age out and remain in the translation table until you enter the **clear** command.

  Conditions: This symptom is observed when the **ip nat outside source static** command is configured in a VRF SNAT environment on a Cisco router that runs Cisco IOS Release 12.4.

  Workaround: If this is an option, use the **ip nat inside source static** command in the VRF SNAT environment.

- CSCsd13124

  Symptoms: A candidate Cisco Bootstrap Router (BSR) that is configured for PIM version 2 and that is elected as a BSR does not change back to a candidate BSR immediately after the BSR interface is shut down but waits until the timer expires. This situation prevents another candidate BSR from becoming a BSR until the first BSR changes back to a candidate BSR when the timer expires.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) but may also affect other releases.

  Workaround: There is no workaround.

- CSCsd15770

  Symptoms: High CPU utilization occurs during PPPoEoQinQ session setup.

  Conditions: This symptom occurs when Internet Group Management Protocol (IGMP) is enabled.

  Workaround: There is no workaround.

- CSCsd16043

  Symptoms: A Cisco IOS platform that is configured for Auto-RP in a multicast environment may periodically lose the RP to group mappings.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(17) when the RP drops the Auto-RP announce messages, which is shown in the output of the **debug ip pim auto-rp** command. This situation may cause a loss of multicast connectivity while the RP mappings are purged from the cache. See the following output example:

  ```
  Auto-RP(0): Received RP-announce, from ourselves (X.X.X.x), ignored
  ```

  Note that the symptom may also affect Cisco IOS Release 12.4 and Release 12.4T.

  Workaround: Create a dummy loopback interface (do not use the configured IP address in the whole network) and use the **ip mtu** to configure the size of the MTU for the RP interface to 1500 and the size of the MTU for the dummy loopback interface to 570, as in the following examples:

  ```
  interface Loopback1
   ip address 10.10.10.10 255.255.255.255
   ip mtu 570
   ip pim sparse-mode
  end
  ```

  (This example assumes that the Auto-RP interface is loopback 0.)

  ```
  interface Loopback0
  ```

```
 ip address 10.255.1.1 255.255.255.255
 ip mtu 1500
 ip pim sparse-dense-mode
end
```

- CSCsd17747

  Symptoms: When you enter the **ip pim vrf register-source** command on an interface and then delete the interface or its IP address, the command remains in the configuration. This situation causes the bulk synchronization to fail and the standby RP to reset continuously after an RP switchover has occurred. Then, because the register source (the interface) cannot be found, a BEM failure occurs.

  Conditions: These symptoms are observed when the interface forwards traffic from a nondefault VRF and when the interface has a register source configured.

  Workaround: Remove the **ip pim vrf register-source** command from the interface before you delete the interface or its IP address.

- CSCsd27388

  Symptoms: A ping from a source to a destination fails because of an encapsulation failure.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for NAT and that has the **ip nat inside source static** command enabled on a VRF.

  Workaround: There is no workaround.

- CSCsd33445

  Symptoms: A Cisco platform that is configured for Next Hop Resolution Protocol (NHRP) may display an error message similar to the following:

  ```
  %SYS-3-MGDTIMER: Running timer, init, timer = 0xXXXXXXXX Process= "NHRP",
  ipl= 0, pid= YYY
  ```

  Conditions: This symptom is observed in a DMVPN environment.

  Workaround: There is no workaround.

- CSCsd48962

  Symptoms: SNAT allocates the “rt_aux_managed_init” string during the first NAT entry creation and a subsequent NAT entry creation triggers the allocation of subsequent memory in NAT and SNAT. When you enter the **clear ip nat trans *** command to free the NAT translation, the rtree memory is not freed, causing a memory leak.

  When you enter the **show processes memory** command, you see that memory is being held but that does not necessarily mean that there is a leak. Only if the held memory is still held upon clearing the NAT table does it mean that there is a leak.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(7.6) and that is configured for SNAT.

  Workaround: There is no workaround.

- CSCsd52667

  Symptoms: When you alter the configuration of the **ip nat pool** command, the router may hang, crash, or both.

  Conditions: This symptom is observed on a Cisco router when you enter the following commands in sequence:

  ```
  ip nat pool address 255.255.255.255 255.255.255.255
  ip nat pool no address 255.255.255.255 255.255.255.255
  ```

  or

no ip nat pool *name*

Workaround: There is no workaround.

- CSCsd64173

  Symptoms: A router may reload unexpectedly because of a bus error crash after you have removed a **summary-prefix** IPv6 OSPF command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF but may also occur in other releases. The symptom occurs only when the **summary-prefix** IPv6 OSPF command is configured without any **redistribute** commands.

  Workaround: Configure a **redistribute** command under the IPv6 OSPF configuration.

- CSCsd67591

  Symptoms: A router may crash when you modify parameters of the **route-map** command for a redistribution statement.

  Conditions: This symptom is observed when you modify the parameters of the **route-map** command for a redistribution statement of an OSPF process that was deleted.

  Workaround: Delete the redistribution statement before you delete the OSPF process.

- CSCsd84489

  Symptoms: A platform that is configured for Open Shortest Path First (OSPF) and incremental Shortest Path First (SPF) may crash when changes occur in the OSPF topology.

  Conditions: This symptom is observed on a Cisco platform that has the **ispf** command enabled when changes occur in the OSPF topology that cause the intra-area routes to be updated.

  Workaround: Disable the **ispf** command.

- CSCuk58462

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- CSCsb89900

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: Corrupted timer data structures may cause tracebacks in an IS-IS environment.

     Condition 1: This symptom is observed when an IS-IS instance is configured for IPv6 interfaces only, when the IS-IS instance has a passive interface, and when you take the following actions:

     – You enter the **no router isis** command.

     – You then re-enable IS-IS, including on the passive interface, which then becomes an active IPv6 interface.

Workaround 1: Do not configure a passive interface if an IS-IS instance is configured for an IPv6 interface only. If you must configure a passive interface in an IS-IS instance, do not enable IS-IS on this passive interface after you have disabled IS-IS at the global via the **no router isis** command.

2. Symptom 2: IS-IS may crash or function unreliably because of uninitialized or freed data structures.

   Condition 2: This symptom is observed when a passive interface is configured and when the following actions occur:

   – IS-IS is disabled on all interfaces (whether IPv4 or IPv6 interfaces), one by one on.

   – Then, the **no router isis** command is entered to disable IS-IS globally.

   – Next, IS-IS is globally enabled and the passive interface is made active via the **ip router isis** or **ipv6 router isis** command.

   Workaround: Do not use a passive interface in an IS-IS environment. If you must use a passive interface in an IS-IS environment, prevent the actions that are described in Condition 2.

- CSCsc63871

  Symptoms: When IS-IS and CLNS are configured, a router may enter a state in which only one adjacency is shown in the output of the **show clns interface** command, even though the **show clns neighbors** command may correctly display all the neighbors that are connected to the interface.

  When this situation occurs and any one of the neighbors on the segment goes down, all routing updates may be lost. The single adjacency is torn down and despite the fact that the output of the **show clns neighbors** command still shows the neighbors, routing stops because there are no adjacencies.

  Conditions: This symptom is observed when an adjacency goes down while it is still in the INIT state. The symptom occurs because the adjacency counter is incorrectly decremented.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.

  Alternate Workaround: Enter the **clear clns neighbors** command on the affected router.

- CSCsd87651

  Symptoms: A Cisco router that is configured for RPR or RPR+ may reload its standby RP when a configuration change is made to IS-IS.

  The reload of the standby RP is proceeded by the following error messages:

  ```
  %HA-3-SYNC_ERROR: Parser no match.
  %HA-5-SYNC_RETRY: Reloading standby and retrying sync operation (retry 1).
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4. Note, however, that the symptom is platform-independent for Release 12.4 and its derivatives. Any of the IS-IS global configuration commands may trigger the symptom. Following are a few examples of these IS-IS global configuration commands:

  - `is-type level-2-only`
  - `lsp-gen-interval level-2 5 50 100`
  - `redistribute eigrp`

  Workaround: There is no workaround.

Miscellaneous

- CSCeb05456

  Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

  ```
  validblock_diagnose, code = 10
  ```

  ```
  current memory block, bp = 0x48FCC7D8,
  memory pool type is Processor
  data check, ptr = 0x48FCC808
  ```

  ```
  next memory block, bp = 0x491AC060,
  memory pool type is Processor
  data check, ptr = 0x491AC090
  ```

  ```
  previous memory block, bp = 0x48FCBBE8,
  memory pool type is Processor
  data check, ptr = 0x48FCBC18
  ```

  The symptom is intermittent and is related to the way NVRAM is accessed.

  Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

  Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

  boot config disk0:
  filename
  nvbypass

- CSCec15400

  Symptoms: A Versatile Interface Processor 4 (VIP4) with an E1 controller may reload unexpectedly and display the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x28, pc=0x604716A8,
  ra=0x604711FC, sp=0x60D66628
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(15)T2, Release 12.2(15)T5, or Release 12.3.

  Workaround: There is no workaround.

- CSCee72997

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCef29090

  Symptoms: The throughput for TCPClear sessions on a Cisco AS5850 may not be as expected and there may be a slow response time.

  Conditions: This symptom is observed on a Cisco AS5850 with TCPclear sessions.

  Workaround: There is no workaround.

- CSCeg03019

  Symptoms: CEF may not work over different tunnels.

Conditions: This symptom has been observed when both GRE and IPIP tunnels are configured and the packet traverses both.

Workaround: There is no workaround.

- CSCeg55213

  Symptoms: Ethernet VLAN data counters may not be updated for a virtual circuit (VC) that is configured for Xconnect.

  Conditions: This symptom is observed on a Cisco platform that has the EoMPLS VLAN mode enabled.

  Workaround: There is no workaround.

- CSCeg86172

  Symptoms: Ports may hang and remain in the "UNREGISTERED" state when you enter the **no sccp** command followed by the **sccp** command.

  Conditions: This symptom is observed when you enter the commands while the ports are in the process of registration to the CME because a switchover has occurred.

  Workaround: Enter the **no stcapp** command followed by the **stcapp** command before you enter the **no sccp** command followed by the **sccp** command. Note that the **no sccp** command removes the protocol stack but does not re-register the ports.

- CSCeh08545

  Symptoms: A router that performs a dynamic DNS update to remove a host name may crash.

  Conditions: This symptom is observed on a Cisco router when an interface that is configured to use dynamic DNS updates and acquire an IP address via DHCP has the **no ip-address** command enabled.

  Workaround: There is no workaround.

- CSCeh22026

  Symptoms: The standby RP of a Cisco 7304 that functions in a high-availability mode may reload unexpectedly.

  Conditions: This symptom is observed under various circumstances, one of which is the following:

  The Cisco 7304 is configured with a port adapter carrier card in which a PA-MC-2T3+ port adapter is installed and you enter the **no channelized** command for one of the ports of the port adapter.

  Workaround: Do not enter the **no channelized** command for a port of the PA-MC-2T3+ port adapter. Rather, configure the startup configuration to include the **no channelized** command for the port of the PA-MC-2T3+ port adapter.

- CSCeh34040

  Symptoms: Incoming traffic is lost when the IP Source Tracker feature is enabled on an interface. A ping times out.

  Conditions: These symptoms are observed when the **ip source-track** command is enabled on a local interface. Even when you enter the **no ip source-track** command, traffic does not resume.

  Workaround: First write down the IP address of the affected interface, then enter the **no ip source-track** command followed by the **no ip address** command on the affected interface, and finally enter the **ip address** command on the affected interface.

- CSCeh60551

  Symptoms: Certain malformed client certificates may cause an Access Point (AP) to crash.

Conditions: This symptom is observed on a Cisco platform that functions as an AP and that runs Cisco IOS Release 12.3(2)JA2 or Release 12.3(4)JA when EAP-TLS is configured. The symptom may also occur in other releases.

Workaround: Issue a new client certificate.

- CSCei05246

  Symptoms: After an OIR of a PA-MC-E3 port adaptor that is installed in a VIP6-80, the serial interfaces do not transmit. The message "not transmitting" is generated, followed by "output frozen." After these messages, a Cbus Complex occurs.

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

  Workaround: There is no workaround.

- CSCei49231

  Symptoms: A router may crash when a large number of calls passes through an E1 CAS link.

  Conditions: This symptom is observed on a Cisco 3800 series that has an E1 CAS link that is configured for E&M wink start signaling.

  Workaround: There is no workaround.

- CSCei86389

  Symptoms: You cannot change the user locale to the RU or NL language.

  Condition: This symptom is observed on a Cisco 7960 IP phone.

  Workaround: There is no workaround. If this is an option for you, use the default user locale, which is the US language.

- CSCej11073

  Symptoms: An attempt to re-enable SSG fails after you have entered the **no ssg enable force-cleanup** command because the SSG unconfiguration process enters an infinite loop.

  Conditions: This symptom is observed on a Cisco router that has about 4000 live sessions.

  Workaround: There is no workaround.

- CSCej27978

  Symptoms: A CE router that is configured for VRFLite does not receive Auto-RP mappings.

  Conditions: This symptom is observed when MDS is enabled on the multilink interface that connects the CE router and the PE router.

  Workaround: Configure process switching on the multilink interface that connects the CE router and the PE router by entering the **no ip mroute-cache** interface configuration command.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek24468

  Symptoms: Dangling bearer channels or voice DSP channels may occur.

  Conditions: This symptom is observed under heavy stress with short duration calls on a Cisco platform such as a Cisco AS5400 or Cisco AS5850 that functions as a gateway.

  Workaround: There are no workaround.

- CSCek24782

  Symptoms: A Cisco platform that is configured for ISDN and AAA may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 5400XM that functions under stress. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCek26044

  Symptoms: The following message may be displayed on the console when you enter the **write memory** command or the **copy nvram:startup-config** command is configured for any SRC configuration:

  NV: Invalid Magic found in NVRAM.....Erase of configuration files recommended

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release 12.4(6.7) or interim Release 12.4(6.6)T and affects the following platforms: Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, Cisco 3845, and a BCM-based Cisco AS5400.

  Workaround: There is no workaround.

- CSCek26158

  Symptoms: A memory leak may occur on a router that is configured for Embedded Event Manager (EEM).

  Conditions: This symptom is observed when EEM Tcl policies are registered to run on the router.

  Workaround: There is no workaround.

- CSCek26311

  Symptoms: A router may crash when certain IP options are changed on a virtual template while PPP sessions are being terminated.

  Conditions: This symptom is observed on a Cisco router when a large number (50,000) of PPP session is being terminated.

  Workaround: Do not change the configuration of the virtual template while a large number of PPP sessions is being terminated.

- 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

- CSCek27156

  Symptoms: The EzVPN connection may fail when you send interesting traffic.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3c).

  Workaround: There is no workaround.

- CSCek27181

  Symptoms: Cisco Land Mobile Radio (LMR) VoIP may not function.

  Conditions: This symptom is observed when multicast if configured.

  Workaround: There is no workaround.

- CSCek27424

  Symptoms: A Cisco 7200 series reloads unexpectedly when you boot the router with Cisco IOS Release 12.4.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for voice.

  Workaround: There is no workaround.

- CSCek29792

  Symptoms: A router that is configured for voice may crash because of a bus error and an error message similar to the following may be generated:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x400BA2B8
  ```

  Conditions: This symptom is observed when all the following conditions occur:

  1. Redirection is triggered by a feature other than Call Forward Busy or Call Forward All.
  2. The calling party such as a user with an FXS phone does not support redirection.
  3. If a TCL script is used, the rerouteMode is set to REDIRECT_ROTARY.
  4. The rerouteNumber is an invalid E.164 number or URL.

  Workaround: There is no workaround.

- CSCek30748

  Symptoms: A router reloads when you enter the **tunnel protection ipsec profile vpnprof** command.

  Conditions: The symptom can be observed on a Cisco 7200 series but may be platform-independent.

  Workaround: There is no workaround.

- CSCek33253

  Symptoms: NextPort modems that function in a T1 CAS signaling configuration do not dial all the DTMF digits successfully.

  Conditions: This symptom is observed when you enter valid DTMF digits such as # and * in a dial string.

  Workaround: Use MICA modems instead of NextPort modems.

  Alternate Workaround: Use ISDN PRI T1 instead of T1 CAS signaling.

- CSCek34049
  - Symptoms: A Cisco AS5850 that is configured for RPR+ may be unable to process more than 1990 MGCP voice calls. With more than 1990 MGCP voice calls, any of the following symptoms may occur:
  - Many DSP may time-out.
  - Active calls may hang.
  - Spurious memory accesses and tracebacks may be generated.
  - Incoming calls may be dropped.
  - NextPort SPE ports may be stuck in the “a” state.

Conditions: These symptoms are observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(3d) or Release 12.4(7a).

Workaround: There is no workaround. A Cisco AS5850 that is used to its full capacity (4 CT3 worth of MGCP calls) may not scale beyond 1990 calls. When the symptoms have occurred, reload the Cisco AS5850.

- CSCek34261

  Symptoms: A Cisco Integrated SONET/SDH Router (ISR) may crash in the "gt96k_mbrd_bri_set_bandwidth" function.

  Conditions: This symptom is observed on a Cisco 1800 series, Cisco 2800 Series, and Cisco 3800 series that function as an ISR when an incoming call is placed with 32 KB bandwidth. Note that the symptom does not occur with a call with 56 KB or 64 KB bandwidth.

  Workaround: Deny the invalid incoming call by entering the **isdn caller** command on the ISR.

- CSCek34617

  Symptoms: A spurious memory access is generated when the router is booting up after a power-cycle or reload.

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3700 series, and Cisco 3800 series that have a virtual asynchronous auxiliary interface configured.

  Workaround: Remove the **interface async1** command from the running configuration and reload the router.

- CSCek35122

  Symptoms: VLAN subinterface counters are not updated for an EoMPLS interface.

  Conditions: This symptom is observed when VLAN packets are switched into a L2VPN Pseudowire Switching environment.

  Workaround: Use Xconnect **show** commands such as the **show mpls l2tr vc detail** command or **show l2tun session all** command to gather information about the VLAN subinterface counters.

  Alternate Workaround: Use pseudowire MIBs to gather information about the VLAN subinterface counters. For example, use the VcPerfTotalInHCBytes (cpwVcPerfTotalInHCBytes) object, which is the equivalent of the ifInOctets input traffic statistic that are not updated for the EoMPLS interface.

- 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

- CSCek37686

  Symptoms: A Cisco AS5350 may reload because of a bus error (SIG=10).

Conditions: This symptom is observed when SNMP is configured and when SNMP queries are made into the Cisco AS5350.

Workaround: Disable SNMP or stop polling the router.

- CSCek38136

  Symptoms: When you deploy VoIP using PVDM2 / 5510 DSP modules, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with 5510 DSP modules. The symptom does not occur with 549 DSP modules.

  Workaround: There is no workaround.

- CSCek38939

  Symptoms: The input error counter may not be incremented for packet errors such as runts, CRC errors, and overrun errors.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1.

  Workaround: There is no workaround.

- CSCin85894

  Symptoms: This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: A "%SYS-3-MGDTIMER" error message followed by a traceback may be generated at the "mgd_timer_complain_uninit" function when an extended ACL is configured with the same name as an active reflexive ACL.

     Condition 1: This symptom is observed when the extended ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the extended ACL.

     Workaround 1: Wait until the reflexive timer expires before you configure an extended ACL with same name as a reflexive ACL.

  2. Symptom 2: A software-forced reload may occur when a standard ACL is configured with the same name as an active reflexive ACL.

     Condition 2: This symptom is observed when the standard ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the standard ACL.

     Workaround 2: Wait until the reflexive timer expires before you configure a standard ACL with same name as a reflexive ACL.

- CSCin86885

  Symptoms: A VIP6-80 in which a PA-MC-STM-1SMI is installed may crash.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release for Release 12.0(31)S after link flaps occur on the PA-MC-STM-1SMI that has QOS configured on its serial interfaces.

  Workaround: There is no workaround.

  Symptoms: When you configure bindings through the **ssg bind direction downlink** global configuration command, the bindings are not applied to interfaces.

  Conditions: This symptom are observed on a Cisco platform that is configured for SSG.

Workaround: Configure bindings through the interface configuration command mode instead of through the global configuration command mode. You can use the following command:

interface type number ssg direction {*downlink* | *uplink*}

Following is an example:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ssg direction downlink
```

- CSCin98933

  Symptoms: When you enter the **write memory**, **copy running-config startup-config**, or **copy** *file* **nvram:startup-config** command, or when the router boots, the router may displays the following error message:

  ```
  NV: Invalid Pointer value(6357F3CC) in private configuration structure
  ```

  Conditions: This symptom is observed under the following conditions:

  1. The router runs Cisco IOS interim Release 12.4(06.05), interim Release 12.4(06.05)T, or later releases, that is, the Cisco IOS image integrates the fix for caveat CSCsc61630.
  2. The error message is generated when the NVRAM is corrupted. This type of NVRAM corruption occurs in rare conditions.
  3. The router is a Cisco 2600 series, Cisco 2800 series, Cisco 3725, Cisco 3745, Cisco 3825, Cisco 3845, Cisco AS5400, Cisco RPM, or Cisco RPM-XF. The symptom does not occur on a Cisco 7200 series or on a Cisco 7500 series that has an RSP.

  Workaround: Enter the **erase nvram:** or **write erase** command to initialize the NVRAM block geometry. Then, enter the **write memory** command to copy the running configuration to the startup configuration. This is a quick, temporary solution. For permanent a solution, see the "Further Problem Description."

  Note: Ensure that you have a backup copy of the startup configuration in some other storage device.

  Alternate Workaround: Save the running configuration to a storage device other than NVRAM.

  Further Problem Description: The symptom occurs because there is a stale, unerased private-configuration pointer in NVRAM, other than the original private-configuration pointer. Because this pointer is an invalid one, the Cisco IOS software image detects this corruption and reports this error.

  When you have upgraded the Cisco IOS software image to one that integrates the fix for caveat CSCin98933, take the following steps:

  1. Create a backup copy of all the required files in NVRAM.
  2. Erase the entire NVRAM by entering the **erase /all nvram:** command, thereby ensuring that there are no stale pointers in NVRAM and that the NVRAM device is filled with 0x0 or 0xFF patterns.
     Note: The **erase nvram:** or **write erase** command erases only the partial contents of NVRAM.
  3. Next, restore the files that were previously in NVRAM back to NVRAM via the **copy** and **write memory** commands.

  In addition, ensure that the Cisco IOS software images that your router is running integrates the fix for caveats CSCin99301 and CSCsd13227 because caveat CSCin98933 may trigger caveats CSCin99301 and CSCsd13227.

- CSCin99301

  Symptoms: The router cannot be reloaded using the **reload** command. The following message is displayed when trying to reload the router:

  ```
  The startup configuration is currently being updated. Try again.
  ```

Conditions: This symptom occurs in some rare conditions. It may be triggered after the "Invalid pointer value in private configuration structure" message is displayed (as seen in CSCin98933 and CSCsd63356).

Workaround: There is no workaround other than power cycling the router.

- CSCsa63173

  Symptoms: CEF may not be updated with a new path label that is received from a BGP peer.

  Conditions: This symptom is observed when a Cisco router that is configured for IPv4 BGP Label Distribution and multipath receives a BGP update that changes only the MPLS label to a non-bestpath multipath. In this situation, the router does not update the forwarding plane, causing dropping or misbranding of traffic because of label inconsistencies between the BGP table and the forwarding table.

  Workaround: There is no workaround.

- CSCsa95310

  Symptoms: For an internally switched ATM link between two RPM blades in a Cisco MGX series, when a PE router blade is connected to another router blade that functions as a Label Switch Controller (LSC), the "physical" sw1.x on the PE router and the XTagNN interface on the LSC may be in the UP state, but an LDP adjacency is never created, preventing traffic from flowing over the ATM interface.

  When the symptom occurs, the output of **show ip interface brief** command on either side of the connection shows that the line is up but the output **show mpls ldp discovery** command does not show any output for the affected ATM interface.

  Conditions: This symptom is observed occasionally when you run automated scripts on the platforms.

  Workaround: When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for the affected ATM interface. Doing so re-enables the traffic to flow.

- CSCsb11565

  Symptoms: On a Cisco CallManager side, only the calling number is seen, and there is no information that the call is a forwarded call.

  Conditions: This symptom is observed when calls are forwarded to a Cisco CallManager by a Cisco Unified CallManager Express (CME) and when the parameter "redirect reason" is incorrectly set.

  Workaround: There is no workaround.

- CSCsb12253

  Symptoms: A Cisco 2600 series may fail to establish a connection with a Cisco CallManager.

  Conditions: This symptom is observed on a Cisco 2600 series that runs Cisco IOS Release 12.4 or Release 12.4T and that is configured for SCCP.

  Workaround: Reboot the Cisco 2600 series.

- 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.

- CSCsb52900

  Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

  Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

  - The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
  - The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

  This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

  Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsb59829

  Symptoms: A Network Admission Control (NAC) device that is associated with a VPN concentrator may prevent a host from accessing the network.

  Conditions: This symptom is observed when the following conditions occur:

  1. A non-Cisco Trust Agent (CTA) host accesses the network with IP address A.
  2. Based on the access policies that the NAC device receives from the Access Control Server (ACS), the NAC device provides access to the non-CTA host.
  3. When the non-CTA host is removed, the same IP address (IP address A) that was associated with the non-CTA host is now assigned to another host.

Workaround: When the hold timer of the NAC device expires, the new host is automatically detected. If the session timeout and termination action are associated with a non-responsive host (NRH), the posture of the new host can be validated during revalidation.

- CSCsb69271

  Symptoms: The voice path confirmation fails due to time-out while waiting for the DTMF tone.

  Conditions: The channels on the CallGen are timed-out waiting for DTMF tones, sent by the other channels. This is not specific to a particular DTMF tone, this is random.

  Workaround: There is no workaround.

- CSCsb71243

  Symptoms: A SIP gateway may not process an incoming REFER request that does not include a "Referred-By" header and turns a "400 Bad Request" response.

  Conditions: This symptom is observed on a Cisco platform that functions as a SIP gateway.

  Workaround: There is no workaround.

  Further Problem Description: RFC3515 does not mandate that a "Referred-By" header is included in a REFER request.

- CSCsb72082

  Symptoms: A router crashes when a call from the PSTN to a SIP gateway is disconnected.

  Conditions: This symptom is observed when the Record-Route header in any message that is received by the gateway is more than 128 bytes long.

  Workaround: Reduce the length of the Record-Route header to less than 128 bytes.

- CSCsb76671

  Symptoms: Intermittent one-way audio (PSTN hears dead air) on inbound ISDN call through Cisco VoIP AS5850 gateway.

  Conditions: This symptom has been observed to occur with inbound ISDN calls with outbound SIP calls towards a Cisco MeetingPlace server. Numerous calls which are transferred via SIP REFER contribute to the gateway get into this state.

  Workaround: There is no workaround to prevent the gateway from getting into this state. Once in this state, reloading the gateway will help clear this condition for awhile.

- CSCsb82045

  Symptoms: Some bindings may not be synchronized when a Cisco router that functions as an active Home Agent R3.0 is reloaded as part of the initial bulk synchronization process.

  Conditions: This symptom is observed only when the **ip mobile home-agent redundancy** *hsrp-group-name* **virtual-network address** *address* command is enabled. This command is required for normal and bulk synchronization of bindings for VRF users. The *address* argument in the command represents the VRF subnet.

  Workaround: Enable redundancy by entering the **ip mobile home-agent redundancy** *hsrp-group-name* command, that is, without the **virtual-network address** keyword and *address* argument.

- CSCsc00038

  Symptoms: A call that is made from an SCCP phone to an analog phone that is connected to a SIP gateway sets up fine. However, when you press the DTMF digits on the SCCP phone, the DSP on a POTS interface crashes.

Conditions: This symptom is observed when the SIP gateway and MTP are configured on the same router, when the SCCP phone and the SIP gateway are registered to a Cisco CallManager, and when the Cisco CallManager inserts MTP into the call.

Workaround: There is no workaround.

- CSCsc04377

  Symptoms: High CPU utilization may occur in the "HTTP CORE" process of a router that is configured for proxy authentication, and proxy authentication attempts may remain in the "INIT" state.

  Conditions: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.3T, Release 12.4, or Release 12.4T.

  Workaround: There is no workaround.

- CSCsc04961

  Symptoms: The **[no] negotiation auto** configuration command causes confusion.

  Conditions: For RJ-45 port on GIgE interfaces, this CLI has no effect. This causes confusion as user(s) are expecting identical behavior between RJ-45 and SFP (i.e. Fibre). To clarify further, according to IEEE, RJ-45 at 1000 Mbps must have Autonegotiation always ON; and that the RJ-45 behavior is undefined if Forced mode is used at 1000 Mbps. Also in case of RJ-45 we always keep Flow Control on by default. Whereas in case of SFP the **[no] negotiation auto** CLI controls Hardware flow-control. This is observed on Cisco IOS Releases 12.3 and also Cisco IOS Release 12.4T. This flow-control feature is further being investigated, and this Release-note may be updated accordingly.

  Workaround: Encourage users to not use this CLI currently when using RJ-45 ports for platform GigE interfaces on Cisco 3825 and Cisco 3845.

  Further Problem Description: The confusion results because this CLI is supported currently only for SFP (i.e. Fibre media). It does two things for SFP:

  1. Sets the mode to either Forced or Autonegotiation depending on [no] option selected or not.
  2. Removes or adds XON/XOFF hardware flow control support depending on [no] option selection.

- CSCsc11636

  Symptoms: A router requires a very long time to boot (more than 5 minutes, potentially hours). Also, changes to the QoS configuration may require long times.

  Conditions: This symptom is observed when the QoS configuration has a complex arrangement of many policies that reference many access control entries (ACEs) through a number of class maps. The time required is, roughly, proportional to the number of combinations of interfaces, policies, classes, and ACEs. For example, if each of 200 interfaces has a QoS policy, each policy uses five class maps, each class map references two ACLs, and each ACL has 30 entries, there are 60,000 combinations.

  Workaround: Either reduce the number of combinations of interfaces, policies, class maps, and ACEs, or load the configuration in two stages. The first stage (from NVRAM) should contain the interface and ACL definitions, and the second stage (from another file) should contain the classes and policies.

- CSCsc11833

  Symptoms: An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

It may take some time for the symptom to occur, but when it does occur, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows you which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

If a problem occur only on a single voice port, there is another problem, not this caveat (CSCsc11833). PRI/BRI calls are no affected because PRI/BRI does not utilize the DSP for signaling purposes,.

When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port-number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41 and 42 is presented and some of the registers show double-octet information. See the example output (2) below.

When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** *port-number* **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

Further Problem Description: When you run a Cisco IOS software image that integrates the fix for this caveat (CSCsc11833) and the symptom still occurs, contact the TAC.

Following are command output examples:

1. Following is an example of normal output for FXO and EVM FXS ports.

   For FXO ports, the value is usually 0x01 but for EVM FXS the value can be different. When you run the above-mentioned command, the expected output is that a single octet is displayed and only for register 39. (This command does not work for VIC-4FXS and VIC2-xFXS modules).

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x01
```

2. Following is an example of output for FXO and EVM FXS ports that indicates that the symptom has occurred. Note that the exact output for the register values is different, but when the symptom occurs, different lines with information are displayed as shown below:

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF
```

3. Following is an example of normal output for FXS and analog E&M modules. The values that are listed in a normal case may be different, but only four registers of a single octet should be displayed.

```
Values read from PEB2465 Codec connected to DSP 02 (channel 0):
---------------------------------------------------------------
Extended Register Values (XR4..XR1) = 00, CC, 50, 11
```

4. Following is an example of output for FXS and analog E&M modules that indicates that the symptom has occurred.

```
Values read from PEB2x65 Codec connected to DSP 0, channel 1:
-------------------------------------------------------------
Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCsc12255

  Symptoms: When you deploy VoIP on an NM-HDV2 network module that is configured with a PVDM2-64 module, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with an NM-HDV2 network module. Note that the symptom does not occur with an NM-HDV network module.

  Workaround: There is no workaround.

- CSCsc12570

  Symptoms: The codec upspeed, for example, from G729 to G711ulaw, or the codec downspeed, for example, from G711ulaw to G729, does not occur. Other call parameter changes that are packet stream-related such as VAD and PLAYOUT do not occur as expected.

  Conditions: This symptom is observed when the codec type or other packet stream parameters are modified by using MDCX or through the TDM side of the call module, via VTSP.

  Workaround: There is no workaround.

- CSCsc14208

  Symptoms: When you change the IP address of a loopback interface that functions as the ID for a TE router, TE auto-mesh tunnels do not reestablish a connection with that router. Also, static TE tunnels for which the destination is modified to match the new loopback IP address cannot reestablish their connection and the tunnels remain down.

  Conditions: This symptom is observed when all of the following conditions occur:

  – OSPF is configured to flood TE advertisements in a given area via the **mpls traffic-eng area** *area-number* command.
  – OSPF is configured to use the loopback interface for which the IP address is modified as the ID for the TE router via the **mpls traffic-eng router-id** *loopback* command.
  – TE tunnels or auto-mesh tunnels are configured with the destination set as the IP address of the loopback interface that is mentioned above.
  – You change the IP address of the loopback interface that is used as the ID for the TE router.

  Workaround: If you need to change the loopback address that is used as the ID for the TE router, follow these steps:

  1. Shut down the loopback interface.
  2. Modify the IP address of the loopback interface.
  3. Bring up the loopback interface.

When the loopback interface address was changed and the symptom has occurred, clear the OSPF routing process in order for the tunnels to be reestablished by entering the **clear ip ospf process** command.

- CSCsc18999

  Symptoms: When you enter the **clear subscriber sessions all** command, the router reloads.

  Conditions: This symptom is observed when Transparent Autologon (TAL) is used with ISG for control over DHCP addressing and when the router is using nearly all available CPU cycles and RAM.

  Workaround: Do not you enter the **clear subscriber sessions all** command.

- CSCsc28313

  Symptoms: Dot1x ports may be unresponsive and ports that are unauthenticated may become stuck unauthenticated.

  Conditions: This symptom is observed when dot1x is configured on more than one routed port and when the line protocol goes down on one of the ports because the remote connection goes down. The remaining ports that are configured for dot1x may become and remain unresponsive until the line protocol on the first port comes back up automatically.

  Workaround: Enter the **no dot1x system-auth-control** followed by the **dot1x system-auth-control** to globally reset the dot1x configuration.

- CSCsc35024

  Symptoms: A Cisco 2600 series with an E1 WIC may crash when you enter the **channel-group timeslots** command.

  Conditions: This symptom is observed when the router runs Cisco IOS Release 12.3(15b) or an earlier release, when a service policy is applied on a subinterface, and when traffic is being processed by the router. The symptom could occur in Release 12.4 or Release 12.4T.

  Workaround: Remove the service policy before you change the time slot.

- CSCsc37281

  Symptoms: TCP connections may not be established between an end device that has TCP stacks that are not RFC-compliant and a platform that has a Cisco IOS firewall enabled.

  Conditions: This symptom is observed when the platform that has the Cisco IOS firewall enabled enforces strict checking for a TCP Window Scale option per RFC1323 section 2.

  Workaround: There is no workaround. Note that the Cisco IOS firewall functions properly.

  Further Problem Description: This is an enhancement request. For Cisco IOS software images that implement this enhancement, the Cisco IOS firewall makes an exception to RFC1323 section 2 so TCP connections can be established between the platform that has the Cisco IOS firewall enabled and an end device has TCP stacks that are not RFC-compliant.

- CSCsc39491

  Symptoms: Cisco Security Monitoring, Analysis, and Response System (MARS) reports a parsing error for the log received from CICS for signature alerts seen on Cisco IOS IPS participating in the Cisco ICS.

  Conditions: MARS is set up to receive events from CICS about signature alerts seen on Cisco IOS IPS participating in ICS.

  Workaround: There is no workaround.

- CSCsc40236

  Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

  Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

  Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc40952

  Symptoms: Phones that are configured for Cisco VT Advantage feature will not register with SRST if they are engaged in SRST fallback operation.

  Conditions: This symptom is observed when using the following:

  – Cisco CallManager Version 5.0 (1.51.225)
  – Cisco 2600 product line for SRST
  – Cisco IOS Release 12.4

  Workaround: Unplug connection to Cisco VT Advantage.

- CSCsc50341

  Symptoms: A router may lose its PVC configuration.

  Conditions: This symptom is observed on a Cisco router that has an IMA group configured on an AIM-ATM on which the **atm bandwidth dynamic** command is enabled. The symptom occurs when the following events occurs:

  1. You use a Telnet session to enter the **show policy-map interface** command for the interface on which the IMA group is configured and the session is waiting for a key stroke at the “more” prompt.
  2. On the far end of the connection, either the T1/E1 cable that provides the connection is pulled out or the **shutdown** command is entered.

  Workaround: There is no workaround.

- CSCsc55822

  Symptoms: There are four different symptoms, all with the same conditions. These symptoms do not occur in any specific order:

  – UDP packets that are smaller than 40 bytes are dropped when the UDP checksum is set to 0.
  – Extended enhanced UDP (Ecudp) packets with a CSRC list are malformed; the “CC” bit is located at the wrong place.
  – When the CSRC list becomes null, the context is not updated to reflect this change.
  – When you enter the **debug ip rtp header-compression** command followed by the **debug ip rtp errors** command, the output may display the wrong packet type. (This situation is of a cosmetic nature.)

  Conditions: These symptoms are observed when you generate UDP packets that are smaller than 40 bytes and when the UDP checksum is set to 0. The UDP packets are generated on a serial interface that has enhanced RTP header compression enabled in IETF format via the **ip rtp header-compression ietf-format** command.

  Workaround for the UDP packets: Send UDP packets that are smaller than 40 bytes with UDP checksums enabled.

  Workaround for the other symptoms: There is no workaround.

- CSCsc58556

  Symptoms: A Cisco router may crash when an EEM Tcl policy runs.

  Conditions: This symptom is observed when the available memory is very low.

  Workaround: Increase the available memory. if this not an option, there is no workaround.

- CSCsc58919

  Symptoms: Packets from a DMVPN tunnel with QoS pre-classification are not classified correctly on the physical interface in the child policy-map of an HQS framework. The access-lists used do not match.

  Conditions: This happens on a Cisco 1841 router running Cisco IOS Release 12.4 (4)T.

  Workaround: There are two possible workarounds:

  - Disable hardware acceleration.
  - Use static crypto-maps in place of DMVPN.

- CSCsc65165

  Symptoms: A Cisco 7200 series reloads unexpectedly when you enter the **hw-module slot** *slot-number* **stop** command for a T3 port adapter.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with 100 EzVPN IVRFs on a DS3 interface of the T3 port adapter.

  Workaround: There is no workaround.

- CSCsc68262

  Symptoms: A Cisco 2821 may crash intermittently.

  Conditions: This symptom is observed on a Cisco 2821 that switches Encapsulating Security Payload (ESP) packets. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsc70644

  Symptoms: User CLI sessions would be stuck on all Cisco routers while configuring QoS.

  Conditions: This symptom has been observed after executing a **show policy-map interface** command with Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsc76061

  Symptoms: When PPPoA and a virtual template are used, ARP requests are not bridged from a LAN through a DSL connection.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(8)YI3 or Release 12.4(4)T when BVI is configured to bridge remote LANs to DSL connections that use PPPoA with virtual templates and aal5ciscoppp encapsulation. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsc76407

  Symptoms: Router-originated packets that are subject to encryption are bypassing the Quality of Service (QoS) feature. This prevents QoS from giving priority to protocol packets (for example BGP), which in turn can cause these protocol packets to be dropped when the outgoing link is congested.

Conditions: This symptom is observed when router-originated packets are IPSec encrypted.

Workaround: Disable CEF and fast switching and use process switching.

- CSCsc79700

  Symptoms: URL filtering takes an excessively long time to revert to the allow mode if a URL Filtering Server is unavailable.

  Conditions: This symptom is observed when a communication loss occurs between the router and the URL Filtering Server because of a failure or an excessive load on the URL Filtering Server, or because of a network connectivity failure between the router and the URL Filtering Server.

  Workaround: There is no workaround.

- CSCsc80670

  Symptoms: When you power-up the router or enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for the on-board Fast Ethernet 0/0 interface, the interface may enter the "FastEthernet0/0 is up, line protocol is down" state.

  Conditions: This symptom is observed when the Fast Ethernet 0/0 interface is connected to particular third-party vendor media converters that are placed in series, as in the following topology:

  ```
  Cisco 1718 (fa0/0) -- media converter<-->media converter --(fa 0/1) Cisco 2950
  ```

  The symptom does not occur when you do not use media converters.

  Workaround: Replace the media converters with those of another third-party vendor. If you need more information, contact the Cisco TAC.

- CSCsc81637

  Symptoms: A Cisco IOS VoIP gateway may reload unexpectedly.

  Conditions: This symptom is observed on a gateway such as a Cisco 2800 series or Cisco 3800 series that supports time-division multiplexing (TDM) hairpinning between voice modules. Under rare circumstances, the gateway may unexpectedly reload when a call is hairpinned between ports on the gateway.

  Workaround: There is no workaround.

- CSCsc83192

  Symptoms: A router may crash when threats are continuously sent and removed from a controller and when simultaneously access control list (ACL) entries are checked by entering the **show ip access-lists** command.

  Conditions: This symptom is observed when an ACL entry is being displayed and when simultaneously the same entry and the next entry are being deleted.

  Workaround: Do not enter the **show ip access-lists** command while a dynamic ACL entry is being deleted.

- CSCsc84858

  Symptoms: A router may crash because of a bus error when you enter the **no policy-map** command.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.3(10c). The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsc85575

  Symptoms: No audio is received from a Cisco 7931 IP phone.

Conditions: This symptom is observed when a call is made between a Cisco 7960 IP phone and a Cisco 7931 IP phone. The user of the Cisco 7960 IP phone experiences one-way audio intermittently while the user of the Cisco 7931 IP phone does not experience this symptom.

Workaround: Reset the Cisco 7931 IP phone.

- CSCsc89979

  Symptoms: When an event is triggered for an EEM applet, a "sequence number out of sync" error message is generated on the router.

  Conditions: This symptom is observed when the "action cli info type cli frequency" command action is defined in the EEM applet.

  Workaround: There is no workaround.

- CSCsc90694

  Symptoms: The standby RP of a Cisco 7500 series may unexpectedly reload.

  Conditions: This symptom is observed when the Cisco 7500 series functions in RPR+ mode and when you perform an OIR of a VIP that is in a disabled analyzed wedged state.

  Workaround: There is no workaround.

- CSCsc90715

  Symptoms: PPPoE sessions are not established.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release version 12.4(6.3) but may also occur in other releases of Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsc90972

  Symptoms: When the DHCP Address Allocation Using Option 82 feature is enabled, multiple classes cannot be given an address range.

  Conditions: This symptom is observed on a Cisco router that has the **ip dhcp class** command enabled.

  Workaround: Follow these steps to assign an address range for multiple classes:

  1. Enter the global configuration mode.
  2. Enter the **ip dhcp pool vlan** global configuration command.
  3. Enter the **class** *classname* command
  4. Configure the address range.

- CSCsc93952

  Symptoms: Only one PRI channel instead of all PRI channels is busied out when Advanced Voice Busy-Out (AVBO) is used.

  Conditions: This symptom is observed on a Cisco router when the **busyout monitor** *interface* command is enabled and when the interface for which the command is enabled is shut down.

  Workaround: There is no workaround.

- CSCsc94359

  Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf** *vrf-name network* command on the PE router that has mismatched labels.

- CSCsc95234

  Symptoms: When the **stcapp** global configuration command is enabled, the command is not accepted and the following error messages are generated:

  ```
  STCAPP: Internal error: Unable to create codec list... exiting stcapp shutdown
  initiated... waiting for calls to clear. stcapp shutdown complete.
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(6.3) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCsc96983

  Symptoms: The following error message is generated and a Gigabit Ethernet interface stops receiving traffic, causing traffic to be dropped:

  ```
  %Y88E8K-3-ILP_MSG_TIMEOUT_ERROR: GigabitEthernet1/0: EtherSwitch Service Module RBCP
  ILP messages timeout
  ```

  Conditions: This symptom is observed on a Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series that are not configured with an inline power supply. Note that the symptom does not occur when the routers are configured with an inline power supply.

  Workaround: There is no workaround. When the symptom has occurred, reload the router to re-enable the router to operate properly.

- CSCsc98158

  Symptoms: When you configure a router as both an EzVPN client and an EzVPN server and when you apply the crypto map to the interface of the router, the EzVPN client connection may fail to complete phase 1. Debugs on the concentrator show retransmissions of the phase-1 packet that is stuck in the “MM_NO_STATE” state. The headend rejects the retransmission because the headend cannot match on a phase 1 retransmission.

  When the EzVPN client attempts to connect to the headend, the EzVPN client transmits only the configured ISAKMP proposals that are meant for the applied crypto map. Because these ISAKMP proposals do no include an “xauth” proposal, the headend rejects these ISAKMP proposals, and the EzVPN client stops transmitting the EzVPN ISAKMP proposals. However, when the crypto map is removed from the interface, the EzVPN client starts to retransmit the EzVPN ISAKMP proposals.

  Conditions: This symptom is observed on a Cisco router that is configured as both an EzVPN client and an EzVPN server and that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsd00206

  Symptoms: Intercepted packets may be switched to a mediation device in the process path.

  Conditions: This symptom is observed on a Cisco platform that is configured for CEF.

  Workaround: Disable CEF switching in order to ensure that packets are switched in the fast path.

- CSCsd01836

  Symptoms: The router crashes when you configure a crypto map in sparse mode.

  Conditions: This symptom is observed on a Cisco router that is configured for IPSec and multicast.

Workaround: There is no workaround.

- CSCsd02602

  Symptoms: All channels on a multichannel T3 port adapter may go down. The router may then reload unexpectedly due to a software forced crash. If not, all of the channels in the T3 may stay down until corrective action is taken.

  The following messages may appear one or more times in the router or VIP log:

  ```
  %CT3-3-MBOXSENDM: Failed to send msg MBOXP_MSG_T1_DISABLE to bay 1 firmware
  ```

  On a Cisco 7200 router, the following messages may be seen in the log:

  ```
  CT3SW WatchDog not cleared, WatchDog = 2
  CT3SW WatchDog not cleared, WatchDog = 3
  ```

  On a Cisco 7500 router, the following messages may be seen in the log:

  ```
  %CT3 5/8: Illegal Love Letter, cmd 0
  %CT3 5/9: Illegal Love Letter, cmd 0
  ```

  Conditions: This symptom affects routers using two-port multichannel T3 port adapters, the PA-MC-2T3 and the PA-MC-2T3+. The symptom occurs when one or more of the T1's in either T3 sees framing errors. One-port multichannel T3 port adapters, the PA-MC-T3 and the PA-MC-T3+, are not affected.

  Workaround: There is no workaround to prevent this problem. Possible corrective actions are listed below:

  Possible Corrective Actions for the Cisco 7200 router:

  1. Remove and reinsert the affected port adapter.
  2. Simulate removal and reinsertion with these exec mode commands in sequence: **hw-module slot** *slot- number* **stop hw-module slot** *slot- number* **start** 3. Reload the router.

  Possible Corrective Actions for the Cisco 7500 router:

  1. Remove and reinsert the VIP with the affected port adapter.
  2. Use the configuration mode command: **microcode reload** 3. Reload the router.

- CSCsd02954

  Symptoms: Some CEF entries are missing from some VRFs, as shown in the output of the **show ip cef inconsistency now** command.

  Conditions: This symptom is observed after an OIR or reload of a Cisco 12000 series GE ISE line card. However, the symptom is not specific to a Cisco 12000 series and may also occur on other platforms.

  Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip cef epoch** command to recover the CEF entries. If this does not recover the CEF entries, enter the **clear ip route vrf** command.

  Further Problem Description: The symptom is observed for local "receive" entries, such as /32 entries for a VRF loopback interface. However, the symptom may also occur for other types of VRF FIB entries.

- CSCsd04075

  Symptoms: A Cisco IOS Voice Over IP Gateway terminating fax calls may have its voice ports lock up and not accept any new calls. The following messages may be seen (but not mandatory) on the console or syslog (if applicable):

  ```
  %HPI-3-CODEC_NOT_LOADED: channel:2/0/0 (171) DSP ID:0x1, command failed as codec not
  loaded 0
  ```

```
- Traceback= 615D2FA8 615C8528 617D5044 617D5258 61BBCD44 61BBD764 617BAE88 617BBD38
6138720C
```

Conditions: This symptom is observed on a Cisco 3600 series router but is not platform dependent.

Workaround: Disabling T.38 and using passthrough resolves the issue.

- CSCsd04665

  Symptoms: A blind transfer of an encrypted intercluster call to an encrypted H.323 gateway causes one-way audio.

  Conditions: This symptom is observed in the following scenario that includes Cisco CallManager 5.0 platforms:

  ```
  Encrypted SIP phone --> CCM1 --> H.323 ICT --> CCM2 --> Encrypted SCCP phone -->
  Encrypted H.323 gateway
  ```

  When a user of the SIP phone calls the SCCP phone and when the user of the SCCP phone performs a blind transfer to the H.323 gateway, the resulting call has one-way audio. The audio exists in the SIP to H.323 direction, but does not exist in the H.323-to-SIP direction. This occurs for encrypted calls only.

  During the blind transfer an open logical channel is sent to the H.323 gateway to establish the media stream from the SIP to H.323 gateway. Later, a close logical channel message followed by an open logical channel message is sent to the gateway to update the media encryption key. At this point, the H.323-to-SIP stream (in the opposite direction from the direction in which the close and open logical channel messages have been sent) is sent to the wrong IP address. It appears to change from being sent to the SIP phone to being sent to the IP address of the CCM1. The change of IP address may be triggered by the "H245Connect" message that follows the close and open logical channel messages.

  Workaround: Disable encryption.

- CSCsd07007

  Symptoms: When a router is booted, the following error message and tracebacks are generated:

  ```
  SYS-2-INTSCHED: sleep for level 3 -Process= Init
  ```

  Conditions: This symptom is observed during initialization of the router with basic configurations after you have loaded the Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsd07033

  Symptoms: A router crashes and generates a traceback at the "p_dequeue" function.

  Conditions: This symptom is observed on a Cisco router when you unconfigure the **pvc range** command.

  Workaround: There is no workaround.

- CSCsd07448

  Symptoms: The output of the **show access-list** command shows that a time-based named extended ACL is not consistent between the RP and a line card.

  Conditions: This symptom is observed when you configure a time range and named extended ACL and when you enter the **ip cef distributed** command.

  Workaround: There is no workaround.

- CSCsd07729

  Symptoms: A router generates the following message:

  ```
  %SSG-5-SSG_TAL_NR: SSG TAL : No response from AAA server. AAA server might be down or
  overloaded.
  ```

A few minutes later, a "%SYS-2-CHUNKBADMAGIC" error causes the router to reload unexpectedly.

Conditions: This symptom is observed on a Cisco router that is configured for SSG.

Possible Workaround: Enter the **no memory lite** command.

- CSCsd08862

  Symptoms: A router may crash because of a bus error when you enter the **show interface** command for a virtual-access interface or subinterface.

  Conditions: This symptom is observed when you enter the **show interface** command while a session that is associated with the virtual-access interface or subinterface is being cleared.

  Workaround: There is no workaround.

- CSCsd09067

  Symptoms: The output of **show policy-map interface** command is not in the expected order: the estimated bandwidth information is placed at the top.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsd10942

  Symptoms: When three or more DN buttons are configured on a Cisco IP Phone Expansion Module 7914 that is attached to a Cisco 7900 series Unified IP phone, one or more DN buttons may get stuck in offhook condition.

  Conditions: This symptom is observed when the DN buttons on the IP phone are randomly and repeatedly pressed.

  Workaround: Reset the IP phone.

- CSCsd10975

  Symptoms: When the error message "duplicate channel names" is seen on the console, the router has to be rebooted to run Embedded Event Manager (EEM) policies again.

  Conditions: This symptom occurs when multiple EEM policies were configured and triggered on a Cisco IOS router. It could lead to the duplicate channel names error.

  Workaround: There is no workaround.

- CSCsd11646

  Symptoms: On a router that runs Multiprotocol Label Switching (MPLS), the "%SYS-3-OVERRUN:" and "%SYS-6-BLKINFO" error messages may be generated and a software-forced crash may occur on the router.

  Conditions: This symptom is observed when you enter the **show mpls ldp discovery** command under the following condition:

  – There are multiple LDP adjacencies configured through one interface.

  – The adjacencies between peers through this interface have not been fully established for some peers.

  – The unestablished LDP adjacencies are coming while you enter the **show mpls ldp discovery** command.

  Workaround: Do not enter the **show mpls ldp discovery** command while multiple LDP adjacencies are coming up. Rather, enter the **show mpls ldp neighbor** [**detail**] command while multiple LDP adjacencies are coming up.

- CSCsd11678

  Symptoms: When you enter the **secure boot-config** command followed by the **secure boot-image** command, and you complete formatting the disk, the output of the **show secure bootset** command does not display the active status.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCsd12941

  Symptoms: The CPU usage may remain at 99 percent for a long time when NMS polls the ipRouteTable via the SNMP protocol.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S or Release 12.0(31)S when there is a large number of routes in the routing table. The symptom may also occur in other releases.

  Workaround: Exclude the ipRouteTable from the SNMP view.

- CSCsd13227

  Symptoms: When saving the current configuration to NVRAM, the following error message is displayed:

  ```
  %Error opening nvram:/startup-config (Device or resource busy)
  ```

  Conditions: This symptom is observed when the router runs Cisco IOS Release 12.4(7), Release 12.4(8)T, or later releases. Enter the **show version** command to detect the Cisco IOS release that is running on the router. This symptom occurs randomly and rarely.

  This symptom may be occur when caveat CSCin98933 is present in the Cisco IOS software image.

  This symptom is observed on the following platforms: Cisco 2600 series, Cisco 2800 series, Cisco 3725, Cisco 3745, Cisco 3825, Cisco 3845, Cisco RPM, Cisco RPMXF cards, and the Cisco AS5400. The symptom does not occur on the Cisco 7200 series and Cisco 7500 series routers with an RSP routers.

  Workaround: Follow these steps:

  1. Create a backup copy of the current configuration on a storage device other than NVRAM.
  2. Reload the router.
  3. Erase the “entire” NVRAM by entering the **erase /all nvram:** command.
  4. Restore the configuration by copying the backup configuration to NVRAM and by entering the **copy startup-config running-config** command.

- CSCsd13419

  Symptoms: A Cisco 3700 series that functions as an RSVP agent may generate a Cisco IOS crash file in flash memory.

  Conditions: This symptom is observed in a topology that includes a Cisco CallManager that is configured for RSVP and two RSVP agents that function as transcoders, one of which is the affected Cisco 3700 series.

  Workaround: There is no workaround.

- CSCsd13920

  Symptoms: CEF switching is broken for voice traffic on some interfaces, which breaks the transcoding feature. The caller then experiences no voice path.

  Conditions: This symptom has been observed on some network modules and interfaces.

Workaround: Disable the **ip cef** command.

- CSCsd14445

  Symptoms: A router crashes when you unconfigure the resource pool of a customer profile.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.4(5b) or Release 12.4(7) and could also occur in Release 12.4T. The symptom may be platform-independent.

  Workaround: Do not unconfigure a customer profile when an active session on the platform uses the customer profile.

- CSCsd15546

  Symptoms: A Cisco router that is configured as a DHCP relay may not append option 82 (that is, the Relay Agent option), even when the router is configured to do so in the following way:

  ```
  ip dhcp relay information option
  no ip dhcp relay information check
  ip dhcp relay information trust-all
  ```

  Conditions: This symptom is observed when the DHCP message contains an invalid option according to RFC 2132; for example, option 12 with length 0.

  Workaround: Ensure that the DHCP messages that are sent to the Cisco router that functions as a DHCP relay contain valid options. If you cannot ensure this, there is no workaround.

- CSCsd16977

  Symptoms: A crash can be observed by segmentation violation (SegV) on a Cisco 2651XM-V-CCME.

  Conditions: This symptom is observed occasionally when a fax is being sent through the router. This problem has been seen with Cisco IOS Releases 12.3(14) T and later versions through Cisco IOS Release 12.4(5).

  Workaround: There is no workaround.

- CSCsd17527

  Symptoms: A Cisco platform that functions as a Cisco CallManager Express (CME) reloads unexpectedly when you create multiple pools.

  Conditions: This symptom is observed on a Cisco 2800 series that functions as a CME. The symptom may be platform-independent.

  Workaround: Do not create multiple pools.

- CSCsd19980

  Symptoms: A router that functions as a DHCP client may crash.

  Conditions: This symptom is observed on a Cisco router when you change the DHCP service through the **ip address dhcp** command or when DHCP is configured more than once.

  Possible Workaround: Before you make any changes, stop the DHCP service by entering the **no ip address dhcp** command followed by the **ip address dhcp** command.

- CSCsd20429

  Symptoms: A router may reload because of a bus error when you enable the SSG TCP Redirect feature.

  Conditions: This symptom is observed when you enable the SSG TCP Redirect feature for unauthenticated user redirection and when there are users being redirected.

  Workaround: There is no workaround.

- CSCsd20733

  Symptoms: FXO ports that are configured for DID and that are controlled by MGCP respond to an AUEP message with an “Endpt Unknown” message.

  Conditions: This symptom is observed when a Cisco router is reloaded or a voice port is configured before a dial peer is configured.

  Workaround: There is no workaround.

- CSCsd24224

  Symptoms: The standby RP reloads unexpectedly because of a synchronization failure.

  Conditions: This symptom is observed when a Stateful Switchover (SSO) occurs and when the **no exception crashinfo file** *device:filename* command is in present in the configuration.

  Workaround: Enable the creation of a diagnostic file by entering the **exception crashinfo file** *device:filename* command.

- CSCsd24311

  Symptoms: SDF files are not loaded onto a router from a TFTP server.

  Conditions: This symptom is observed with any NAT mode (static, dynamic, overload, or off) and with either fast switching, flow switching, or CEF switching configured.

  Workaround: There is no workaround.

- CSCsd25758

  Symptoms: A router may crash when you run an SNMP query for the CiscoCBQosMIB.

  Conditions: This symptom is observed on a Cisco router that has IP Header Compression (IPHC) in the Class-Based Weighted Fair Queueing (CBWFQ) configuration.

  Workaround: There is no workaround.

- CSCsd27683

  Symptoms: An H.323 gateway may not initiate an H.245 TCP connection, and a call may be dropped unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that functions as an H.323 gateway and that runs Cisco IOS Release 12.4(7) when the terminating gateway or Cisco CallManager sends an Alert message with an H.245 address and a Progress Indicator (PI) of 1,2,8 in its response to a fast start setup message.

  Workaround: Configure “progress_ind alert strip” on the outgoing dial peer.

  Alternate Workaround: Enter the **call start slow** command under the voice service VoIP H.323 mode as shown below:

  ```
  voice service voip
   h323
    call start slow
  ```

  Further Problem Description: When an H.323 gateway initiates a fast start call to another gateway or Cisco CallManager, the terminating gateway or Cisco CallManager sends a slow start Alert message with an H.245 address and a PI of 1,2,8. The user of the phone that connects to the originating gateway expects a ringing tone from the terminating gateway, but does not hear a ringing tone, even though the phone that is connected to the terminating gateway does ring. When the phone that is connected to the terminating gateway is not picked up (and, therefore, no Connect message is sent), the call is dropped. The symptom does not occur when there is no PI in the Alert message.

- CSCsd29308

  Symptoms: The NAS port value is not incorrect in RADIUS packets, that is the access-requests and accounting requests are incorrect.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG and occurs for QinQ users over an IP connection.

  Workaround: There is no workaround.

- CSCsd29364

  Symptoms: Service Selection Gateway (SSG) does not send attribute NAS-PORT [5] on the access request packet for a prepaid service reauthorization.

  Conditions: This symptom occurs when SSG is configured, and User is a prepaid user.

  Workaround: There is no workaround.

- CSCsd30244

  Symptoms: The router crashes on busyout of a CT3 card.

  Conditions: This symptom has been observed only after the router is booted with no T1 configuration on the T3 controller.

  Workaround: There is no workaround.

- CSCsd30533

  Symptoms: Duplicate IPsec flows may be created on the responder side during IPsec Quick Mode (QM) negotiation, leaving one flow with IPsec SAs and the other flow empty. This situation may cause multiple IPsec SAs to be created.

  Conditions: This symptom is observed during the creation of IPsec SAs when the IPsec module fails to find the existing flow.

  Workaround: There is no workaround.

- CSCsd31198

  Symptoms: Packets may exceed the PCR, causing large packets to be dropped by an ATM switch.

  Conditions: This symptom is observed when a VBR-nrt PVC is configured on an NM-1A-OC3-POM network module with the PCR identical to the SCR and when the cell delay variation tolerance (CDVT) is violated at low traffic rates. The symptom may also occur when a CBR PVC is configured on an NM-1A-OC3-POM network module.

  Workaround: Set the SCR to a slightly lower value than the PCR or do not configure a CBR PVC. Verify that the SCR and PCR settings are correct by entering the **show controller atm** *slot/port* command and ensuring that the SCR is a value other than 0, as in the following command output example:

  ```
  Tx bytes (489890600), Tx packets (360325), PCR/SCR (10240/10230)
  ```

- CSCsd33134

  Symptoms: A router reloads unexpectedly when HTTP client sockets hang.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T2, or a later release, including Release 12.4 and Release 12.4T, when VXML is used to play long audio prompts that are streaming from an HTTP server.

  Workaround: Enter the **ivr prompt streamed none** command on the router.

- CSCsd35474

  Symptoms: A router may crash during the certificate upgrade process for a Cisco Unified IP Phone that is registered to a Cisco Unified Call Manager Express.

  Conditions: This symptom is observed on a Cisco router, is platform-independent, and relates to the Public Key Infrastructure (PKI).

  Workaround: There is no workaround.

- CSCsd35555

  Symptoms: The TDM crossconnect for a T1/E1 WIC does not function.

  Conditions: This symptom is observed on a Cisco IAD 2400 series that is configured with a VIC2-2MFT-T1/E1 WIC.

  Workaround: Use the native T1/E1 slot to install the WIC in.

- CSCsd38247

  Symptoms: A router that is configured with IP tunnels may crash and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: This symptom is observed on a Cisco router when you enter the **default keepalive 3 5** command on a tunnel interface.

  Workaround: There is no workaround.

- CSCsd38693

  Symptoms: Renaming a file to a string that contains multiple trailing dots (“.” characters) corrupts the file system on ATA, CF, and USB flash storage devices.

  Conditions: This symptom is observed when you enter the following commands to rename the file:

  ```
  rename disk0:file2 disk0:file3...
  ```

  Workaround: Avoid renaming a file that contains multiple trailing “.” characters. When the symptom has occurred and the file system is no longer accessible, you must reformat the disk by entering the **format disk0:** command.

- CSCsd39519

  Symptoms: A Media Gateway Control Protocol (MGCP) gateway hangs when voice calls come in from either the IP or the PSTN side in which a leg of the call is on a BRI Voice Interface Card (VIC). The gateway stops responding and does not process any traffic. The only way to bring the router back is to power-cycle it.

  Conditions: This symptom is observed for every call over a BRI VIC/WIC if the MGCP gateway runs Cisco IOS Release 12.4(4)T1 or later releases. The symptom may also occur in Release 12.4.

  Workaround: There is no workaround. The symptom is not observed when the MGCP gateway runs Cisco IOS Release 12.4(4)T.

- CSCsd40153

  Symptoms: An ASBR has “No Label” as its outgoing label for a peer ASBR interface address.

  Conditions: This symptom is observed when the following conditions occur:

  - An ISP network (ISP network A) has two ASBRs that peer with one ASBR in another ISP network (ISP network B).
  - IGP routing (OSPF or any other IGP) is configured between the ASBRs in ISP network A.
  - A BGP session between one ASBR in ISP network A and the ASBR in ISP network B flaps.

  - After about 5 minutes, all routes that are reachable via the ASBRs in ISP network A and the ASBR in ISP network B have “No Label” as their outgoing label.

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

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd41070

  Symptoms: Calls are dropped because of a backhaul link failure during a switchover of a Cisco PGW 2200 Softswitch.

  Conditions: This symptom is observed on a redundant Cisco PGW 2200 Softswitch system that is connected to a Cisco AS5850 and that is configured for MGCP-controlled PRI backhaul. Calls drop after the switchover of the Cisco PGW 2200 Softswitch because there is a disconnect between the Layer 2 and the D channel.

  Workaround: There is no workaround.

- CSCsd43706

  Symptoms: A Cisco router crashes while executing the **show policy-map interface** command.

  Conditions: Configure the service policy with CBWFQ and WRED based on prec and Explicit Congestion Notification (ECN).

  Workaround: There is no workaround.

- CSCsd44118

  Symptoms: When running TCL/VXML applications that perform Media Play, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: This symptom is observed when Cisco IOS Media Play code forgets to release a memory at the end of Media Play.

  Workaround: There is no workaround. Contact Multiservices TAC (IOS) and request a patch.

- CSCsd46323

  Symptoms: The standby RP reboots when you perform an OIR of an active VIP that is installed in any slot of the router.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.4(7.10) and that is configured for RPR, RPR+, or SSO. The symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCsd46403

  Symptoms: When a call enters an E1 R2 line on a Cisco platform and is sent via an H.323 link to an endpoint, the endpoint does connect the call but the Cisco platform does not send a “TX ANSWERED” message on the CAS leg, causing a dead air condition for the call.

Conditions: This symptom is observed on a Cisco AS5350, Cisco AS5350XM, Cisco AS5400, and Cisco AS5400XM that run a Cisco release later than Cisco IOS Release 12.3(11)T9. The symptom may also occur in other releases.

Workaround: There is no a workaround.

- CSCsd46569

  Symptoms: It may take 10 seconds before a first call-waiting tone is played instead of being played immediately. If this situation occurs, the subsequent tones are played every 10 seconds.

  Conditions: This symptom is observed on a Cisco router that functions as a CME and that runs Cisco IOS Release 12.4 or Release 12.4T. The symptom occurs with either firmware version 7.2(2) or version 7.2(4).

  Workaround: There is no workaround.

- CSCsd47734

  Symptoms: A memory leak may occur when you run an EEM Tcl policy.

  Conditions: This symptom is platform- and release-independent.

  Workaround: There is no workaround.

- CSCsd51429

  Symptoms: A Cisco router that is running SNASw that has lost connectivity on an HPR-IP link shows the link state as active with the **show snasw link** command. The message "%SNASW-4-LDLC_CTRL_LOG_1: EXCEPTION - 81 - LDLC command frame retry limit exceeded" appears, but a message "%SNASW- 3-EVENT: Link station XXXX deactivated" does not. The mainframe product correctly shows the link as inactive.

  The link cannot be reactivated. Trying to stop the link with the **snasw stop link** command leaves the link in Pending Inactive state.

  Conditions: This symptom occurs when there is an outage between the SNASw router and the mainframe, such as an IP failure, interface failure, or mainframe reload.

  Workaround: There is no workaround. The SNASw subsystem must be restarted with the **snasw stop** command followed by the **snasw start** command to clear the condition.

  Further Problem Description: This problem was caused by a bad code fix in CSCej78434.

- CSCsd56683

  Symptoms: When you leave a voice mail for an IP phone that is not registered, the MWI light does not come on when the IP phone reregisters.

  Conditions: This symptom is observed on a Cisco device that is configured for Cisco Unified CallManager Express (CME).

  Workaround: There is no workaround.

- CSCsd58220

  Symptoms: The callee's phone rings continuously even after the caller goes on- hook.

  Conditions: When the caller goes on-hook, the gateway receives idle and does not recognize the idle. The call does not get disconnected and the callee keeps hearing the ringing tone continuously.

  Workaround: The callee has to pick up the phone for the call to be dropped.

- CSCsd58381

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd61780

  Symptoms: A router crashes because of errors from checkheaps.

  Conditions: This symptom is observed when hundreds of CLI commands are entered in virtual-template mode.

  Workaround: There is no workaround.

- CSCsd64304

  Symptoms: A router crashes and generates a traceback when you attempt to import certificates.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(7.15) but may also occur in Release 12.4T.

  Workaround: There is no workaround.

- CSCsd65549

  Symptoms: SSH sessions are not established.

  Condition: This symptom is observed when you attempt to make an SSH connection to a Cisco router that is configured for SSH version 1.

  Workaround: There is no workaround.

- CSCsd65602

  Symptoms: The MGCP state may change to “Shutting Down” when you unconfigure MGCP after a COT-related call has been made.

  Conditions: This symptom is observed on a Cisco router when you enter the **no mgcp** command.

  Workaround: There is no workaround.

- CSCsd67958

  Symptoms: A router that functions as a Home Agent (HA) and that is configured for PIM may crash when a neighbor with a higher Layer 3 address attempts to become the Designated Router (DR).

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(7.15) and that functions as an HA when the following conditions are present:

  – The Mobile IP HA feature creates and deletes mobile IP tunnels.
  – The interfaces on the HA and its neighbor are configured for sparse-dense mode PIM.

  The symptom may also occur in other releases.

  Workaround: If PIM must be configured on the tunnel interfaces, select high values for the tunnel interface numbers to prevent the Mobile IP HA feature from using the same numbers for the mobile IP tunnels.

  Alternate Workaround: Configure PIM on the tunnel interfaces before the Mobile IP HA feature creates any mobile IP tunnels.

- CSCsd72965

  Symptoms: A ping between two WIC-2T WAN Interface Cards (WICs) that are connected back-to-back fails at 8 MHz in V.35 mode.

Conditions: This symptom is observed on a Cisco 2610XM and Cisco 2611XM that are connected back-to-back via WIC-2T WICs when the clock rate is configured to function at 8 MHz in V.35 mode.

Workaround: There is no workaround.

Further Problem Description: Even though the clock rate is configured to function at 8 MHz, both the Cisco 2610XM and the Cisco 2611XM generate a clock rate of 9.7 Mhz.

- CSCsd73749

  Symptoms: Traffic that is processed by PVCs with a small bandwidth on an NM-1M-OC3-POM network module may encounter large latencies and may be dropped from the output queue.

  Conditions: This symptom is observed on a Cisco router that is configured with an NM-1A-OC3-POM network module when the PVCs have a small bandwidth that is less than 10 Mbps.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat provides the following solution:

  On ATM line cards, the SAR mechanism has a queue for each PVC. Two thresholds are associated with each PVC queue: the high watermark and low watermark. The high watermark defines the number of cells that the queue can hold.

  The watermark values are used to apply a flow control mechanism between the host and the SAR on the NM-1A-OC3POM network module. When cells start backing up in the SAR, the SAR sends a notification to the host as soon as the queue inside the SAR builds up to a high watermark. At this point, the VC is marked as throttled and packets start backing up in the Cisco IOS software hold queues. At the same time, the SAR is draining out the packets. When the SAR reaches the low watermark, another notification is sent to the host. The VC is marked as “Open” and traffic to the VC resumes. The problem is caused by the low values that are configured for the high and low watermarks on the SAR.

  To configure watermark values that are suitable for your applications, use the **queue-depth** command, which is available in a Cisco IOS software image that integrates the fix for caveat CSCsd73749.

  The command syntax and usage are explained below:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int atm 1/0
Router(config-if)#pvc 1/1
Router(config-if-atm-vc)#queue-depth ?
<1-65535>  queue depth high watermark, in cells

Router(config-if-atm-vc)#queue-depth 200 ?
<1-200>  queue depth low watermark, in cells

Router(config-if-atm-vc)#queue-depth 200 100 ?
<cr>

Router(config-if-atm-vc)#queue-depth 200 100
Router(config-if-atm-vc)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

  Note that the default values of watermarks are not changed in a Cisco IOS software image that integrates the fix for caveat CSCsd73740.

  Guidelines for configuring the watermarks are as follows:

A high watermark translates into larger queue build-up inside the SAR, affecting the latency of LLQ-type traffic. A low watermark translates into the use of the traffic shaping mechanism within the SAR. If a low watermark is too low, the SAR may drain its queue entirely, causing a breakage of traffic shaping.

In general, if you need to change the watermark values, follow these guidelines:

- For better latency, decrease the high watermark value.
- For a higher number of cells in the queue or for better TCP performance, increase the high watermark value.
- Do not configure the low watermark value to be equal to the high watermark value because this defeats the purpose of the flow control mechanism.
- Even though the **queue-depth** command allows a high watermark value up to 65535, we do not recommended that you configure such a high watermark value. A high watermark value translates into queues within the SAR. How high the value of the high watermark can be is defined by the SAR memory. For example, with 1024 VCs, when the high watermark is configured above 400 cells, the SAR may run out of memory, causing packet drops to occur.
- Detailed guidelines about high and low watermark values will be provided in a separate document. As a rough guideline, default values of high and low watermarks for PVCs with a bandwidth of less than 1 Mbps are 50 and 10. The symptom may occur with these values. However, when you multiply these values by a factor of 4 via the **queue-depth** command such that the new values are 200 and 40, the symptom no longer occurs.

- CSCsd74000

  Symptoms: A slot controller such as a slot controller of a VIP4-80 may reset because of a TLB (load or instruction fetch) exception.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(17b) or Release 12.4, that has T1 or E1 port adapters installed in the slot that is controlled by the slot controller that resets, and that has NBAR configured.

  Workaround: Remove the NBAR configuration.

- CSCsd77724

  Symptoms: A router that is configured as a Service Selection Gateway (SSG) and that has the TCP Redirect feature enabled may reload unexpectedly.

  Conditions: This symptom is observed under a rare condition when there are multiple unauthenticated TCP Redirect mappings on an interface and when the SSG subblock of this interface goes down.

  Workaround: There is no workaround.

- CSCsd79558

  Symptoms: When tunnel protection is configured on a tunnel interface, an IPSec session may fail to come up.

  Conditions: This symptom is observed when the **tunnel vrf** *vrf-name* command is changed on the tunnel interface.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove and re-add the tunnel interface.

- CSCsd79879

  Symptoms: Reverse Route injection for IPSec in an EzVPN server and EzVPN client may remove routes from existing connections.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or a release up to and including interim Release 12.4(7.8) when the following conditions are present:

- There are dynamic clients in a VRF environment.
- The **reverse-route remote-peer** *ip-address* command is configured underneath a dynamic map.
- The remote peer changes its IP address.

The combination of the above-mentioned conditions causes a situation in which the old SA remains from the previous IP address while there is also a new SA. When the old SA times out, the refcount decrements to zero, causing the RRI entry to be removed from the table of the EzVPN server. At this time, both the EzVPN server and the EzVPN client have IPSec SAs and could send traffic, but the EzVPN server cannot correctly route the traffic.

Workaround: Clear the IPSec SAs for the EzVPN server. When the EzVPN server reconnects, a new RRI entry is created.

Alternate Workaround: If this is an option, remove the **reverse-route remote-peer** *ip-address* command.

- CSCsd98525

  Symptoms: An SSH version 2 (SSHv2) session is terminated prematurely.

  Conditions: This symptom is observed when large chunks of data are transferred in the SSHv2 session, for example, when the **show tech** command is entered and the command output is transferred in the SSHv2 session.

  Workaround: Use SSH version 1.

- CSCse01143

  Symptoms: IPC does not function after an RPR+ switchover has occurred,

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for RPR+ and dLFIoLL.

  Workaround: Reload the microcode onto the router.

- CSCse01847

  Symptoms: When agentless hosts are allowed network access, a loss of connectivity may occur during reauthentication.

  Conditions: This symptom is observed when the host does not have a Cisco Trust Agent (CTA) configured.

  Workaround: There is no workaround.

  Further Problem Description: When an agentless host is authorized for network access, a dynamic access policy is applied for the host. This access policy is removed at the beginning of the reauthentication process, and re-applied at the end of reauthentication process. During the reauthentication process, no access policy is applied for the host. This situation may cause a disruption to network access.

- CSCse17317

  Symptoms: A Cisco router crash is observed while testing E1R2 test for different country codes and codecs.

  Conditions: This problem is seen while using E1R2 digital semi-compelled signaling only.

  Workaround: There is no workaround.

- 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.

TCP/IP Host-Mode Services

- CSCee73956

  Symptoms: The Generalized TTL Security Mechanism (GTSM), formerly known as BGP TTL Security Hack (BTSH), checks the time-to-live (TTL) value of the packets at the application level, which is not efficient. Also, GTSM does not stop the establishment of a TCP connection for a packet with an invalid TTL value.

  Conditions: This symptom is observed on a Cisco platform that has the **neighbor** *neighbor-address* **security ttl hops** *hop-count* command configured in a BGP environment.

  Workaround: There is no workaround.

- CSCek12203

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

  Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

  Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

Wide-Area Networking

- CSCed51827

  Symptoms: When you ping a router, the following error message is generated on the router:

  ```
  %IPFAST-2-PAKSTICK: Corrupted pak header for Virtual-Access3, flags 0x80
  ```

  Conditions: This symptom is observed when PPP Multilink (MLP) over L2TP is configured.

  Workaround: There is no workaround.

- CSCeh64479

  Symptoms: A router reloads unexpectedly when an apparent Layer Two Forwarding (L2F) packet is received.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Virtual Private Dialup Network (VPDN). However, the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCej20215

  Symptoms: Calls could not be placed once the router was upgraded from Cisco IOS Release 12.3(14)T to Cisco IOS Release 12.4(3).

Conditions: This symptom has been observed with Cisco IOS 12.4(3) and placing calls using the E1 EuroISDN link.

Workaround: Install Cisco IOS Release 12.3(14)T.

- CSCek17486

  Symptoms: When you attempt to place a call over an ISDN BRI interface that is not yet up, the router reloads with the following stack decode:

```
0x61a2a698:etext(0x610a5790)+0x984f08
0x603344dc:gt96k_mbrd_bri_set_bandwidth(0x603343dc)+0x100
0x6011e298:bri_isdn_set_bandwidth(0x6011e1f8)+0xa0
0x61a2a698:etext(0x610a5790)+0x984f08
0x6011e298:bri_isdn_set_bandwidth(0x6011e1f8)+0xa0
0x61a2a6b8:etext(0x610a5790)+0x984f28 0x6042da28:host_connect(0x6042d500)+0x528
0x61a2a728:etext(0x610a5790)+0x984f98 0x6043bf7c:process_rxstate(0x6043b9a8)+0x5d4
0x61a2a790:etext(0x610a5790)+0x985000 0x60426500:Host_Start(0x604264f0)+0x10
```

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsc67930. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc67930. 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.

- CSCek25684

  Symptoms: When you remove a map group from an interface, the router may reload.

  Conditions: This symptom is observed while Frame Relay SVC is coming up.

  Workaround: Shut down the interface before you remove the map group from the configuration.

- CSCek28575

  Symptoms: A router reloads at the "process_modem_command" function during a test that involves asynchronous media.

  Conditions: This symptom is observed on a Cisco AS5400 but is not platform-dependent.

  Workaround: There is no workaround.

- CSCek31660

  Symptoms: For VPDN sessions that are established with a LAC, the RADIUS progress code in the Stop record may be different from the RADIUS progress code in the Start record.

  Condition: This symptom is observed on a Cisco platform such as a Cisco AS5400 that runs Cisco IOS Release 12.4.(3a) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCsb64662

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: Multicast packets that traverse a Frame Relay virtual circuit (VC) bundle are dropped.

     Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

     Workaround 1: There is no workaround.

  2. Symptom 2: Multicast packets that traverse a Frame Relay virtual circuit (VC) bundle are process-switched.

     Condition 2: This symptom is observed with Cisco IOS Release 12.3.

Workaround 2: There is no workaround.

- CSCsc89546

  Symptoms: An L2TP tunnel comes up on a shutdown loopback interface.

  Conditions: This symptom is observed when an L2TP tunnel is initiated on a shutdown loopback interface.

  Workaround: There is no workaround.

- CSCsc93002

  Symptoms: When configuring transparent bridging of IP over Frame Relay, MAC entries are not seen in the ARP-cache.

  Conditions: The symptom has been observed when sending ping packets through the transparent bridge over Frame Relay between the end systems.

  Workaround: There is no workaround.

- CSCsc95588

  Symptoms: A Cisco router reloads when you enter the **show log**, **show interface**, or **show caller** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(5b) but may occur in any Cisco IOS 12.3 release and in other releases as well. The symptom may occur when PPP sessions go down while the output of a **show** command is suspended.

  Workaround: There is no workaround.

- CSCsd01816

  Symptoms: Multilink interfaces do not recover after a T1 link in a bundle flaps.

  Conditions: This symptom is observed when two Cisco router are connected back-to-back via two channelized OC-3 connections with 168 T1 links and when the multilink bundles are created with two T1 links each.

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

- CSCsd06510

  Symptoms: Unexpected drops may occur in the Multilink Frame Relay (MFR) output hold queue. The drops persist under a very low (25 pps) transmit rate.

  The MFR output hold queue may become congested, causing all traffic to fail.

  After you have disabled the traffic source or shut down the ingress interface, the MFR output hold queue may take as long as 15 minutes to “drain.”

  Conditions: These symptoms are observed on a Cisco router when you run multicast traffic over GRE tunnel interfaces that in turn use an MFR interface for transport.

  Workaround: Disable multicast fast-switching.

- CSCsd11874

  Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an MFR interface when the bundle links are down, the serial interfaces that are associated with the MFR interface remain in the IDLE state.

  Conditions: This symptom is observed on a Cisco router that is configure for MFR.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on each serial interface that is associated with the MFR interface.

- CSCsd28564

  Symptoms: When adding or removing PPP over Frame Relay (PPPoFR) configuration on a Cisco 7500 series router, the following error message is displayed:

  ```
  %RSP-3-RESTART: cbus complex
  ```

  Conditions: This symptom occurs on a Cisco 7500 series router when PPPoFR configuration is added or removed.

  Workaround: There is no workaround.

- CSCsd42088

  Symptoms: A router may become unresponsive and crash during bootup, and %SYS-3-CPUHOG errors message may be generated for the Frame Relay ARP process.

  Conditions: This symptom is observed on a Cisco router that has the **ip address dynamic** command enabled on a Frame Relay subinterface that is connected to a peer that also has the **ip address dynamic** command enabled.

  Workaround: Because the configuration that is described in the Conditions is an invalid configuration, ensure that the peer has a valid IP address when the **ip address dynamic** command is enabled on the router.

- CSCsd47777

  Symptoms: Any PPP session that runs on a subinterface may crash.

  Conditions: This symptom is observed with PPPoA, PPPoE, or VPDN sessions on a subinterface.

  Workaround: Enter the **no virtual-template subinterface** command globally.

- CSCsd51082

  Symptoms: An ISDN Layer 2 may not become active after a failure.

  Conditions: This symptom is observed when ISDN backhaul is configured.

  Workaround: There is no workaround.

- CSCsd74130

  Symptoms: When an HSSIRSET, SERRSET, or FDDIRSET error message is generated or when the output becomes stuck, a VIP does not come up during its first recovery attempt.

  Conditions: This symptom is observed on a Cisco platform that is configured with a VIP when a CCB timeout occurs during an IDB reset or when the output becomes stuck.

  Workaround: There is no workaround.

- CSCsd79611

  Symptoms: L2TP sessions are not established when multihop is configured.

  Conditions: This symptom is observed when SGBP is configured in a multihop environment. The L2TP sessions fail to be established because the source IP address is marked as down.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7h)

Cisco IOS Release 12.4(7h) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7h) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCsk35985

  Symptoms: The system crashes when the **show ipv6 ospf lsdb-radix** hidden command is entered.

  Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

Miscellaneous

- CSCsc93952

  Symptoms: Only one PRI channel instead of all PRI channels is busied out when Advanced Voice Busy-Out (AVBO) is used.

  Conditions: This symptom is observed on a Cisco router when the **busyout monitor** *interface* command is enabled and when the interface for which the command is enabled is shut down.

  Workaround: There is no workaround.

- CSCsh74975

  Symptoms: A router may reload or a leak memory may occur when UDP malformed packets are sent to port 2517.

  Conditions: This symptom is observed on a Cisco router that functions as a VoIP dial peer and that is configured for H.323.

  Workaround: There is no workaround.

- CSCsi81891

  Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

  Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

  Workaround: There is no workaround.

- CSCsj96577

  Symptoms: A Cisco AS5400HPX crashes due to a bus error as indicated by show version “System returned to ROM by bus error at PC 0x61728370, address 0xB0D0B45”.

  Just before the crash the following error message is seen:

  ```
  %SYS-2-NOTQ: unqueue didn't find 674D6D40 in queue 3C -Process= "MGCP
  Application", ipl= 0, pid= 170
  ```

  Conditions: This symptom is observed on a Cisco AS5400HPX.

  Workaround: There is no workaround.

- CSCsk00177

  Symptoms: GRE traffic needs to be specifically allowed in the outside interface terminating DMVPN IPSec protected traffic.

  Conditions: This symptom is observed on a DMVPN tunnel interface with tunnel protection IPSec, with CEF or fastswitching.

  Workaround: - use process switching. - allow the GRE traffic.

- CSCsk10985

  Symptoms: IMA group interface does not come up after the reload.

Conditions: This symptom is observed on a Cisco 2811 router with ATM interface that is using VWIC2-2MFT-T1/E1 connected to MGX AUSUM card.

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

TCP/IP Host-Mode Services

- CSCsh92986

  Symptoms: The latency for the **RSH** command could increase when they are flowing through an FWSM module.

  Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

  Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3 which is not affected by this extra delay issue.

Resolved Caveats—Cisco IOS Release 12.4(7g)

Cisco IOS Release 12.4(7g) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7g) but may be open in previous Cisco IOS releases.

- CSCdz55178

  Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

  Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                         00000000011111111111222222222333^
                         12345678901234567890123456789012|
                                                          |
                                                   PROBLEM
                                                 (Variable Overflowed).
```

  Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCsj38829

  Symptoms: When running double auth crypto (ah encap and esp encap auth together) configurations and passing large packet data which requires fragmentation, errored packets can be observed.

  Conditions: This symptom has been observed on routers with AIM-VPN-PLUS AIM cards installed. Routers which support this AIM are Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 routers.

  Workaround: Do not use ESP and AH double authentication, or use the **no crytpo engine accel** command in the configuration to run encryption in the software engine.

- CSCsj52667

  Symptoms: The gateway in SRST gets IP phones registered and it attempts to register them to the gateway as E.164 numbers.

Conditions: The attempt to register fails if GK has zone prefix already pointing in the direction of Cisco CallManager, so new E.164 numbers are overlapping with that zone prefix and pointing to the different zone where the GW originally is.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7f)

Cisco IOS Release 12.4(7f) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7f) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsf32390

  Symptoms: When tuning particle clone, F/S, and header pools after these were made configurable via CSCuk47328, the commands may be lost on a reload.

  Conditions: If the device is reloaded the commands are not parsed on a reload and this results in the defaults being active. This may result in traffic loss if the increased buffers were needed to enable greater forwarding performance for the specific network design.

  Workaround: Configure an applet to enter the buffer values again after a reload. A sample applet would be:

  event manager applet add-buffer

  event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"

  action 1.0 cli command "enable"

  action 2.0 cli command "configure terminal"

  action 3.0 cli command "buffers particle-clone 16384"

  action 4.0 cli command "buffers header 4096"

  action 5.0 cli command "buffers fastswitching 8192"

  action 6.0 syslog msg "Reinstated buffers command"

- CSCsj44081

  Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  Details:

  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.

  Recommended Action

  Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization.

IP Routing Protocols

- CSCek47667

  Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

  Workaround: There is no workaround.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

  Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  Workaround: Add area 0 in the OSPF VRF processes.

  Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

Miscellaneous

- CSCds25257

  Symptoms: A gatekeeper rejects new registration requests from a Cisco Unified CallManager (CUCM) or other H.323 endpoints with Registration Rejection (RRJ) reason of duplicateAlias. Attempting to clear this stale registration fails and a “No such local endpoint is registered, clear failed.” error message is generated.

  Conditions: This symptom is observed in the following topology:

CUCM H.225 trunks register to a gatekeeper (GK) cluster. Gatekeeper 1 (GK1) and gatekeeper 2 (GK2) are members of the GK cluster. The CUCM registers first to GK1, then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

When the H.225 trunk attempts to register with GK1, it is rejected because the alternate registration is still present, and there is no way to clear it.

```
10.9.20.3       34273 10.9.20.3       32853 SJC-LMPVA-GK-1    H323-GW A
    ENDPOINT-ID: 450FC24400000000  VERSION: 5  AGE: 1618993 secs
SupportsAnnexE: FALSE
    g_supp_prots: 0x00000050
    H323-ID: SJC-LMPVA-Trunk_4
```

Workaround: Reset the gatekeeper by entering the **shutdown** command followed by the **no shutdown** command, or reboot the affected GK.

- CSCek38201

  Symptoms: A router may reload or display an alignment traceback when you enter the **show crypto socket** command.

  Conditions: This symptom is observed on a Cisco router that has an OSPFv3 IPSecv6 configuration.

  Workaround: There is no workaround. To prevent the symptom from occurring, do not enter the **show crypto socket** command in an OSPFv3 IPSecv6 configuration.

- CSCek55486

  Symptoms: The native Gigabit Ethernet (GE) interface on an NPE-G1 card may reset unexpectedly.

  Conditions: This symptom is observed on a Cisco 7200 series when the underrun counter for the native GE interface increments continuously. You can verify the underrun counter in the output of the **show interfaces gigabitethernet** *slot/port* command.

  Workaround: There is no workaround.

- 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.

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t


  ip ssh version 1
  ```

```
end

Alternate Workaround: Permit only known trusted hosts and/or networks to
connect to the router by creating a vty access list, as in the following
example:

10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any

line vty 0 4
access-class 99 in
end
```

Further Problem Description:

For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6350_TSD_Products_Configuration_Guide_Chapter.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/warp/public/707/ssh.shtml

- CSCsf08998

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

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

- 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

- CSCsg96319

  Symptoms: When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:***number ip-address* command.

  Conditions: This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhanmt_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  Workaround: Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- CSCsg99814

  Symptoms: On a router that functions in a GRE over IPSec or Virtual Tunnel Interface (VTI) configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface.

  Conditions: This symptom is observed when the ACL on the tunnel interface is configured on the outbound physical interface on which the IPSec tunnel is terminated.

  Workaround: Apply the outbound ACL on the protected LAN interface instead of on the tunnel interface.

- CSCsh33430

  Symptoms: A traceback may occur in an HSRP function and the platform may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that has the HSRP Support for ICMP Redirects feature enabled and occurs when a learned HSRP group is removed after a resign message has been received.

  Workaround: Disable the Support for ICMP Redirects feature by entering the **no standby redirects** global configuration command.

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

```
%MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of
[dec] - VRF [chars]
```

Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

Workaround: There is no workaround.

- CSCsh75827

  Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the "J" Service-Info attribute), has logged out from the SESM, and then renews its IP address.

  Workaround: There is no workaround.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi27540

  Symptoms: A VSI session may become stuck in the "RESYNC_UNDERWAY" state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

  Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

  Workaround: There is no workaround.

- 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

- CSCsi67763

  The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

  http://www.kb.cert.org/vuls/id/739224

  By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

  Cisco response is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml

- CSCsi84017

  Symptoms: When you reload a Cisco 2600 series, the router may hang.

  Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCsh06841

  Symptoms: A router may crash while establishing a PPP session.

  Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

  Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsh82513

  Symptoms: The output of the **show isdn active** command may show disconnected calls.

  Conditions: This symptom is observed on a Cisco router when analog modem calls are made after a normal ISDN digital call has been made.

  Workaround: There is no workaround.

- CSCsi74960

  Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

  Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

  Workaround: There is no workaround.

- CSCsj10593

  Symptoms: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(15.6) and that functions as a TGW with all PRI switch types from the user to the network side. The symptom occurs when the **isdn test call interf ace** *interface-number dialing-string* command is entered at the platform on which the call is initiated, when the originating gateway (OGW) is configured for the National ISDN (primary-ni) switch type, and when the TGW is configured for the NT DMS-100 (primary-dms100) switch type. The symptom may also affect Release 12.4T.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7e)

Cisco IOS Release 12.4(7e) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7e) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCse66080

  Symptoms: A memory leak may occur in the Entity MIB API process.

  Conditions: This symptom is observed when an entity is registered with the same name as an entity that is already registered.

  Workaround: There is no workaround.

- CSCsg21398

  Symptoms: Cisco IOS may restart when receiving a crafted TACACS+ msg-auth-response-get-user packet after it sends out an initial TACACS+ recv-auth-start packet.

  Conditions: This symptom has been observed with TACACS+ packets.

  Workaround: There is no workaround.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

IP Routing Protocols

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- CSCse04037

  Symptoms: A ping or a Telnet connection from an inside gateway to an outside gateway through a router that is configured for NAT may fail because of an error in the NAT table lookup process.

  Conditions: This symptom is observed on a Cisco router when the **preserve-port** keyword is not configured in the **ip nat service** command and occurs whether or not NAT Overload is configured.

  Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsg00860

  Symptoms: Enabling NAT outside on the public interface terminates the VPN connection as GREoverIPSEC. Inbound ACL applied on the public interface starts to drop decrypted GRE traffic.

  Conditions: This symptom has been observed with the use of IP NAT outside on the public VPN interface.

  Workaround: There are two workarounds:

  1. Configure NAT translations for all traffic, to force NAT processing on the packet even if no address will actually be translated. Example:

     ```
     ip nat inside source static 171.16.68.5 171.16.68.5
     ```

     It is not a scalable workaround but may work for some deployments.

  2. Configure an additional ACL entry in the inbound access-list to permit the incoming GRE traffic.

- CSCsh80678

  Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(22) or a later release when the **auto-summary** command is enabled for BGP.

  Workaround: Enter the **no auto-summary** command.

Miscellaneous

- CSCei49231

  Symptoms: A router may crash when a large number of calls passes through an E1 CAS link.

Conditions: This symptom is observed on a Cisco 3800 series that has an E1 CAS link that is configured for E&M wink start signaling.

Workaround: There is no workaround.

- CSCek26311

  Symptoms: A router may crash when certain IP options are changed on a virtual template while PPP sessions are being terminated.

  Conditions: This symptom is observed on a Cisco router when a large number (50,000) of PPP session is being terminated.

  Workaround: Do not change the configuration of the virtual template while a large number of PPP sessions is being terminated.

- CSCek45344

  Symptoms: A Cisco AS5400XM gateway crashes after 24 hour stress with E1-R2 calls.

  Conditions: This symptom occurs in stress conditions after a period of 24 hours.

  Workaround: There is no workaround.

- CSCek47653

  Symptoms: A voice gateway may crash because of a bus error that is related to an MGCP Visual Message Waiting Indicator (VMWI) function.

  Conditions: This symptom is observed on a Cisco IAD 2430 that runs Cisco IOS Release 12.3(14)T2. The symptom may also affect Release 12.4 and Release 12.4T.

  Workaround: There is no workaround.

- 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.

- CSCsc84858

  Symptoms: A router may crash because of a bus error when you enter the **no policy-map** command.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.3(10c). The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd28214

  Symptoms: A Cisco router that is running Cisco IOS Release 12.3(19) may crash due to a Watch Dog timeout while running the RIP routing protocol.

  Conditions: The router may crash due to a Watch Dog timeout if an interface changes state at the exact same time a RIP route learned on that interface is being replaced with a better metric redistributed route. For example, RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0. If RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, then the RIP route will be removed. If, during this time the Fast Ethernet 1/0 interface goes down, then the router may potentially crash due to a Watch Dog timeout.

  Workaround: There is no workaround.

- 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.

- 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

- 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.

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- CSCse91102

  Symptoms: A Cisco IAD 2430 IAD crashes on Cisco IOS Release 12.4(4)T2. Traceback decodes indicate memory corruption. The following events may also appear in the log:

  ```
  %SYS-3-BADMAGIC: Corrupt block at %SYS-6-MTRACE: mallocfree: addr, pc
  %SYS-6-BLKINFO: Corrupted magic value in in-use block %SYS-6-MEMDUMP:
  ```

  Conditions: The router crashes where the decodes indicate check heaps as the source with any or all of the following also included in decode:

  ```
  crashdump validblock validate_memory checkheaps checkheaps_process
  ```

  Workaround: There is no workaround.

- CSCsg15598

  The Intrusion Prevention System (IPS) feature set of Cisco IOSÆ contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.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.

- CSCsg59326

  Symptoms: When an ATM (that is, a cash machine, not a WAN platform) is connected to a switch service module, significant packet loss may occur.

  Conditions: This symptom is observed on a Cisco 2800 series router.

  Workaround: Change the Ethernet speed to 10 Mbps at both ends.

- CSCsg76715

  Symptoms: A device crashes when you delete an ACE that was inserted in the middle of the ACL rather than added at the end of the list.

  Conditions: This symptom is observed when all of the following conditions are present:

  – The inserted ACE has a destination prefix length of 0, that is, is has an “any” statement instead of a destination address.

  – The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an “any” statement), and the inserted ACE has a lower sequence number than this other ACE.

  – The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

  Workaround: First, delete the inserted ACE. Then, delete the other ACE with the same SRC prefix length and an destination prefix length that is greater than 0.

  Alternate Workaround: Delete the complete ACL.

- CSCsh20092

  Symptoms: The value that is defined in the **config-register** *value* command may unexpectedly change on the standby eRSC.

  Conditions: This symptom is observed on a Cisco AS5850 when you boot the eRSCs in RPR+ mode.

  Workaround: There is no workaround.

- CSCsh58082

  Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

  There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

  Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsh94526

  Symptoms: When an acct-stop message is received for a non-RADIUS proxy user (that is, a normal IP user), a router that is configured for SSG crashes.

  Conditions: This symptom is observed when SSG is configured for RADIUS proxy mode and when the **ssg wlan reconnect** command is enabled.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCse81069

  Symptoms: Unconfiguring the **isdn service b_channel** command is not taking effect. The command is not removed from the running configuration.

  Conditions: This symptom occurs when configuring the **isdn service b_channel** command to a state other than the default value of 0 on the ISDN D channel.

  Workaround: To remove the command, shut down the T1/E1 controller first and then unconfigure the command under the D channel serial interface.

- CSCsf30493

  Symptoms: When a T.37 onramp call is made, the following error message may be generated:

  ```
  %CSM-3-NO_VDEV: No modems associated
  ```

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS interim Release 12.4(10.7). The symptom may not be platform-specific.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7d)

Cisco IOS Release 12.4(7d) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7d) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCir00074

  Symptoms: A router crashes when the casnDisconnect object is set to “true” for a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series when you attempt to terminate the PPPoE session through SNMP by using the casnDisconnect object of the CISCO-AAA-SESSION-MIB.

  Workaround: There is no workaround.

- CSCsf19139

  Symptoms: %RADIUS-3-NOSERVERS messages are logged after a reload in Cisco IOS Release 12.3(18). At this time, the RADIUS accounting tickets are not generated.

  Conditions: This symptom has been observed on a Cisco AS5300 gateway.

  Workaround: Enter into configuration mode and change the order of the servers under the server group.

- CSCsg03830

  Symptoms: The **tacacs-server directed-request** command appears in the running configuration when is should be disabled. When you disable the command by entering **no tacacs-server directed-request** and reload the router, the command appears to be enabled once more.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for CSCsa45148, which disables the **tacacs-server directed-request** command by default.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa45148. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Temporary Workaround: Each time after you have reloaded the router, disable the command by entering **no tacacs-server directed-request**.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  – Reload the router.

  – A switchover of the active RP occurs.

  – Enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCsa87034

  Symptoms: When you attempt to clear the routing table, the neighbor is brought down instead.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 unicast *** or **clear bgp ipv6 unicast *** command, causing respectively the IPv4 neighbor or IPv6 neighbor to be brought down.

  Workaround: There is no workaround.

- CSCsc52732

  Symptoms: When PIM is enabled or disabled on a subinterface, multicast traffic that is received on another subinterface of the same main interface is dropped for a moment.

  Conditions: This symptom is observed on a Cisco router that is configured for IP Multicast. The higher the multicast traffic rate is, the more packets are dropped.

  Workaround: There is no workaround.

- CSCse98590

  Symptoms: The router will display SYS-2-MALLOCFAIL messages on the console, and various protocols will operate erratically as a result of a low memory condition.

  Conditions: When a router has to duplicate incoming IPv4 multicast packets for transmission on multiple interfaces, and one of those interfaces is a GRE tunnel operating in GRE IPv6 mode, then memory used to duplicate that packet stream will not be freed. As a result, the router will soon exhaust all available memory.

  Workaround: The router will not exhaust memory if packets do not need to be duplicated (for example, if they enter on one interface and only exit the box through another interface), or if they do not need to duplicate to a tunnel interface that is running GRE over IPv6 (for example, tunnel mode GRE IPv4 does not have this problem).

ISO CLNS

- CSCse85158

  Symptoms: Locally advertised networks that are configured for the NSAP address- family under BGP will not be readvertised once they have been cleared from the BGP table.

  Conditions: Once the **clear bgp nsap unicast *** command has been issued, the networks will no longer appear in the output of the **show bgp nsap unicast** command.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb05456

  Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

```
validblock_diagnose, code = 10

 current memory block, bp = 0x48FCC7D8,
 memory pool type is Processor
 data check, ptr = 0x48FCC808

 next memory block, bp = 0x491AC060,
 memory pool type is Processor
 data check, ptr = 0x491AC090

 previous memory block, bp = 0x48FCBBE8,
 memory pool type is Processor
 data check, ptr = 0x48FCBC18
```

  The symptom is intermittent and is related to the way NVRAM is accessed.

  Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

  Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

  boot config disk0:

  filename

  nvbypass

- CSCed57504

  Symptoms: A router reloads when a session using virtual-template configuration and terminated on this router is being cleared from the DSL CPE router that is the peer router for the connection.

  Workaround: There is no workaround.

- CSCeg86867

  Symptoms: An AAA server does not authenticate.

Conditions: This symptom is observed on a Cisco platform that functions as an AAA server and that runs Cisco IOS Release 12.3(13) when you dial up using Microsoft callback through an asynchronous line. Dialup through an ISDN modem works fine.

Workaround: There is no workaround.

- CSCek48251

  Symptoms: When you enter the **redundancy switch-activity force** command on the active eRSC of a Cisco AS5850 while incoming VoIP H.323 calls and outgoing CAS calls are being processed, the standy eRSC does become the active eRSC and processes the calls but soon afterwards may crash at "csm_enter_idle_state."

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(9)T and that functions in RPR+ mode. The symptom may also affect Release 12.4.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRI calls are being processed.

- CSCek55511

  Symptoms: A Cisco AS5400HPX that is running Cisco IOS Release 12.3(11)T7 may crash with IO Memory corruption.

  Conditions: The crash may occur when polling for ccrpCPVGEntry, and resource pooling is enabled on the Gateway.

  Workaround: Disable SNMP polling for ccrpCPVGEntry.

- CSCek57655

  Symptoms: A modem autoconfiguration fails.

  Conditions: This symptom is observed in an asynchronous call.

  Workaround: There is no workaround.

- CSCin99565

  Symptoms: A router that is configured for SSG may reload unexpectedly.

  Conditions: This symptom is observed when both the Transparent Auto-Logon (TAL) and Port-Bundle Host-Key (PBHK) SSG features are enabled and when it takes a long time before the AAA server responds.

  Workaround: There is no workaround.

- CSCsb11565

  Symptoms: On a Cisco CallManager side, only the calling number is seen, and there is no information that the call is a forwarded call.

  Conditions: This symptom is observed when calls are forwarded to a Cisco CallManager by a Cisco Unified CallManager Express (CME) and when the parameter "redirect reason" is incorrectly set.

  Workaround: There is no workaround.

- CSCsb12253

  Symptoms: A Cisco 2600 series may fail to establish a connection with a Cisco CallManager.

  Conditions: This symptom is observed on a Cisco 2600 series that runs Cisco IOS Release 12.4 or Release 12.4T and that is configured for SCCP.

  Workaround: Reboot the Cisco 2600 series.

- CSCsb71243

  Symptoms: A SIP gateway may not process an incoming REFER request that does not include a "Referred-By" header and turns a "400 Bad Request" response.

  Conditions: This symptom is observed on a Cisco platform that functions as a SIP gateway.

  Workaround: There is no workaround.

  Further Problem Description: RFC3515 does not mandate that a "Referred-By" header is included in a REFER request.

- CSCsc96983

  Symptoms: The following error message is generated and a Gigabit Ethernet interface stops receiving traffic, causing traffic to be dropped:

  ```
  %Y88E8K-3-ILP_MSG_TIMEOUT_ERROR: GigabitEthernet1/0: EtherSwitch Service Module RBCP
  ILP messages timeout
  ```

  Conditions: This symptom is observed on a Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series that are not configured with an inline power supply. Note that the symptom does not occur when the routers are configured with an inline power supply.

  Workaround: There is no workaround. When the symptom has occurred, reload the router to re-enable the router to operate properly.

- CSCsd04075

  Symptoms: The voice ports of a Cisco IOS Voice over IP (VoIP) gateway that terminates fax calls may lock up and not accept any new calls. The following error messages may be generated on the console or syslog (if enabled):

  ```
  %HPI-3-CODEC_NOT_LOADED: channel:2/0/0 (171) DSP ID:0x1, command failed as codec not
  loaded 0
  ```

  ```
  - Traceback= 615D2FA8 615C8528 617D5044 617D5258 61BBCD44 61BBD764 617BAE88 617BBD38
  6138720C
  ```

  Conditions: This symptom is observed on a Cisco 3600 series router but is not platform-dependent.

  Workaround: Disable T.38 and use fax passthrough.

- CSCsd04665

  Symptoms: A blind transfer of an encrypted intercluster call to an encrypted H.323 gateway causes one-way audio.

  Conditions: This symptom is observed in the following scenario that includes Cisco CallManager 5.0 platforms:

  ```
  Encrypted SIP phone --> CCM1 --> H.323 ICT --> CCM2 -->
  ```

  ```
  Encrypted SCCP phone --> Encrypted H.323 gateway
  ```

  When a user of the SIP phone calls the SCCP phone and when the user of the SCCP phone performs a blind transfer to the H.323 gateway, the resulting call has one-way audio. The audio exists in the SIP to H.323 direction, but does not exist in the H.323-to-SIP direction. This occurs for encrypted calls only.

  During the blind transfer an open logical channel is sent to the H.323 gateway to establish the media stream from the SIP to H.323 gateway. Later, a close logical channel message followed by an open logical channel message is sent to the gateway to update the media encryption key. At this point, the H.323-to-SIP stream (in the opposite direction from the direction in which the close and open logical channel messages have been sent) is sent to the wrong IP address. It appears to change from being sent to the SIP phone to being sent to the IP address of the CCM1. The change of IP address may be triggered by the "H245Connect" message that follows the close and open logical channel messages.

Workaround: Disable encryption.

- CSCsd09067

  Symptoms: The output of **show policy-map interface** command is not in the expected order: the estimated bandwidth information is placed at the top.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsd10942

  Symptoms: When three or more DN buttons are configured on a Cisco IP Phone Expansion Module 7914 that is attached to a Cisco 7900 series Unified IP phone, one or more DN buttons may get stuck in offhook condition.

  Conditions: This symptom is observed when the DN buttons on the IP phone are randomly and repeatedly pressed.

  Workaround: Reset the IP phone.

- CSCsd15968

  Symptoms: MGCP seems to be sourcing media from a different interface than what is configured under the **mgcp bind media source- interface** *interface-id* command.

  Conditions: This symptom has been observed when using a Cisco IOS MGCP gateway going to any MGCP call agent and the MGCP traffic bound to an interface that is using the **ip address negotiated** command - meaning the IP address is learned dynamically via IPCP / BOOTP.

  Workaround: Bind the MGCP traffic to an interface that has a static IP address defined on it.

- CSCsd20733

  Symptoms: FXO ports that are configured for DID and that are controlled by MGCP respond to an AUEP message with an “Endpt Unknown” message.

  Conditions: This symptom is observed when a Cisco router is reloaded or a voice port is configured before a dial peer is configured.

  Workaround: There is no workaround.

- CSCsd34529

  Symptoms: A Cisco router may crash when a policy map is simultaneously displayed and unconfigured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T but may also affect Release 12.4. The symptom occurs when the **show policy-map** command is entered via one CLI session while the **no policy-map** *policy-map-name* command is entered via another CLI session.

  Workaround: There is no workaround.

- CSCsd38247

  Symptoms: A router that is configured with IP tunnels may crash and generate the following error message:

  ```
  "%ALIGN-1-FATAL: Illegal access to a low address"
  ```

  Conditions: This symptom is observed on a Cisco router when you enter the **default keepalive 3 5** command on a tunnel interface.

  Workaround: There is no workaround.

- CSCsd46569

  Symptoms: It may take 10 seconds before a first call-waiting tone is played instead of being played immediately. If this situation occurs, the subsequent tones are played every 10 seconds.

  Conditions: This symptom is observed on a Cisco router that functions as a CME and that runs Cisco IOS Release 12.4 or Release 12.4T. The symptom occurs with either firmware version 7.2(2) or version 7.2(4).

  Workaround: There is no workaround.

- CSCsd56683

  Symptoms: When you leave a voice mail for an IP phone that is not registered, the MWI light does not come on when the IP phone reregisters.

  Conditions: This symptom is observed on a Cisco device that is configured for Cisco Unified CallManager Express (CME).

  Workaround: There is no workaround.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  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.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

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

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.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.

- CSCse03855

  Symptoms: An IP phone display remains stuck at “Enter Number” for the duration of an outgoing call to the PSTN.

  Conditions: This symptom is observed when the IP phone runs CME version 3.3 and is connected to a BRI ISDN interface on a Cisco router that runs Cisco IOS Release 12.4. When you enable the **debug isdn q931** command, the following message is displayed in response to an outgoing setup message:

```
ISDN BR0/2/0 Q931: RX <- SETUP_ACK pd = 8  callref = 0x83
Channel ID i = 0x89
```

  Progress Ind i = 0x8288 - In-band info or appropriate now available Workaround: Prevent the Telco from sending the following information in the setup_ack message:

```
Progress Ind i = 0x8288 - In-band" information or appropriate now available
```

  Note that the symptom does not occur in Cisco IOS Release 12.3(11)T10 and with CME version 3.2.

- CSCse18355

  Symptoms: A Cisco AS5850-ERSC gateway reboots continuously with the message:

```
Bundled Rommon and FPGA versions are different from
 the current system version. Updating the system.
 This might take a while
```

```
System reload is required before upgrade can be done.
Rebooting the system ..
!
```

Conditions: This symptom has been observed when a Cisco AS5850-ERSC gateway is running Cisco IOS interim Release 12.4(7.24)T.COMP.

Workaround: Boot to ROM monitor mode and enter the following commands:

```
SKIP_UPGRADE=1
sync
```

This step skips the upgrade process. To revert back, enter the following commands:

```
unset SKIP_UPGRADE
sync
```

- CSCse39452

  Symptoms: OGW rejects incoming OLC from an alternate endpoint when the slow start procedure is used and so the call is rejected.

  Conditions: This symptom has been observed when OGW is configured to use the slow start procedure.

  Workaround: There is no workaround.

  Further Problem Description: OGW is configured to use the slow start procedure. OGW receives alternate endpoints in the ACF. The call on the primary endpoint fails after H.245 procedures are completed and logical channel are opened. Now OGW tries the call on alternate endpoint, but it rejects the incoming OLC from the alternate endpoint, thus resulting in call failure.

- CSCse42141

  Symptoms: T38 fax calls fail when they come inbound through DID Analog ports. In the debug h245 asn1, there is no OLCAck sent back towards the fax server.

  Conditions: This symptom was only reproduced on analog ports. PRI works with the same configuration.

  Workaround: Send the fax call through a PRI.

- CSCse49985

  Symptoms: A software-forced crash may occur on a Cisco 3745, and an error message similar to the following may be displayed:

  ```
  rcojx67-vgw01-3745 uptime is 1 day, 16 hours, 19 minutes
  System returned to ROM by error - a Software forced crash, PC 0x60A87D38
  at 15:59:36 GMT Tue May 16 2006
  System restarted at 16:00:35 GMT Tue May 16 2006
  System image file is "flash:c3745-ipvoice-mz.123-14.T3.bin"
  ```

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(14)T3 only when there are some memory allocation failures. The symptom may also affect Release 12.4.

  Workaround: There is no workaround.

- CSCse50887

  Symptoms: MGCP IOS Gateway sees the following:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  and then:

  ```
  config term router(UNKNOWN-MODE)
  ```

Or, the **show running-config** command output is only 5 bytes.

Conditions: This symptom occurs under the following conditions:

- Use MGCP with the **ccm-manager config** command
- Have more than 20 MGCP end points (voice ports)
- Run Cisco IOS 12.3(11)T or later releases
- Reset device pool from Cisco CallManager

Workaround: Add the **no ccm-manager config** command.

- CSCse89402

  Symptoms: The CPU stack frame may become corrupted when a channel-group is configured on the T1/E1 controller.

  Conditions: This symptom is seen on mainboard WIC slots when the slot is configured for the "no network-clock participate."

  Workaround: Use the VWIC in "network-clock participate" when installed in the mainboard WIC slot of the router.

  Further Problem Description: In most situations, no problems are seen. In rare cases, a crash may occur.

- CSCsf03530

  Symptoms: A crash occurs on a router when it receives a message waiting indicator (MWI).

  Conditions: This symptom is observed when unity sends a notify to the gateway (GW), and the GW is suppose to convert to QSIG MWI. The GW crashes while running Cisco IOS Interim 12.4(9.18)T.

  Workaround: There is no workaround.

- 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

- CSCsf31178

  Symptoms: HWIC-1GE-SFP may experience an issue where the Gig Ethernet interface is "stuck" in a Line UP/Protocol Down state. While in this state, the interface will not pass traffic. Clearing the interface or manually disabling/enabling will clear the condition. This symptom does not occur when 1000BASE-T SFP is used.

  Conditions: A Loss of Signal (for example, unplugging the cable) may cause the interface to become stuck in a Line UP/Protocol Down state.

  Workaround: Clearing the interface or manually shutting it down, then bringing it back up will clear the problem.

- CSCsf95938

  Symptoms: There is a leak in middle buffers after all Onboard DSPRM Pools are depleted.

  Conditions: This symptom is observed on a Cisco 3800 series router that is running Cisco IOS Release 12.4(7b) with support for CVP survivability.

  Workaround: There is no workaround.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsg00602

  Symptoms: A Cisco 3845 or Cisco 3825 router with AIM-VPN/HPII-PLUS(EPII-PLUS) may show the following symptoms: 1) show alignment errors 2) crash by bus error 3) XXX display by running the **show crypto engine accel ring packet** command 4) if a telnet session, which shows symptom three, is cut by "clear line," its related exec process does not disappear and starts to occupy CPU.

  Conditions: This failure is seen on the Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco 1800 series routers that are configured with an AIM-VPNII or AIM-VPNII PLUS Virtual Private Network (VPN) encryption and hardware advanced integration module (AIM).

  Workaround: Avoid running the **show crypto engine accel ring packet** command.

- CSCsg05350

  Symptoms: A Cisco AS5850 crashes due to a chunk memory leak. See the following:

  ```
  Sep  9 13:07:04.428: %DSMP-3-INTERNAL: Internal Error : NO MEMORY -Traceback=
  0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50 0x6127F6BC
  Sep  9 13:07:04.468: %DSMP-3-INTERNAL: Internal Error : NO MEMORY -Traceback=
  0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50 0x6127F6BC
  Sep  9 13:07:04.744: %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a
  reload due to Fragmented processor_memory, Free processor_memory = 10402472
  bytes, Largest processor_memory block = 522632 bytes
  ```

  Conditions: This symptom occurs when there is a chunk memory leak.

  Workaround: There is no workaround.

- CSCsg07907

  Symptoms: A Cisco 3845 router unexpectedly reloads with bus error as seen in the show version when enabling DSP mini logger (voice dsp <slot> command history enable).

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4 with conferencing enabled on the DSP slot that minilogger is being turned on for.

  Workaround: Disable conferencing on that slot, if possible.

- CSCsg11718

  Symptoms: A VRF may become stuck in the "Delete Pending" state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- 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.

- CSCsg18933

  Symptoms: A RIP route is learned from a RIP neighbor via a dialer interface (or other virtual interface type). When the neighbor disconnects and the interface goes down, the RIP route is removed from the RIP database. However, the RIP route remains in the routing table.

  Conditions:

  – RIP is configured with the **no validate-update-source** command.
  – RIP routes are learned via a virtual interface.
  – The virtual interface is using a negotiated address.
  – The problem is platform-independent.

  Workaround: Use the **clear ip route** command to remove the affected routes from the routing table.

- CSCsg28628

  Symptoms: NAS pkg asynchronous calls fail after a redundancy switchover has occurred, and the following error message is generated:

  Modems unavailable

  Conditions: This symptom is observed on a Cisco AS5850 that functions in RPR+ mode. This situation may impact service.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **redundancy switchover** command a couple of times to restore the Cisco AS5850 to normal operation.

- CSCsg84883

  Symptoms: NAT configurations are not getting removed.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Interim Release 12.4(12.3)T.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCek12203

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

- CSCse05736

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

  Conditions: This symptom is seen under the following conditions: 1. The router must have RCP enabled. 2. The packet must come from the source address of the designated system configured to send RCP packets to the router. 3. 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.

Wide-Area Networking

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP.

  Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCek59078

  Symptoms: An L2TPv3 session is established when voluntary tunneling is configured and both peers have corresponding configurations. However, after configuring the pseudowire on UUT virtual-PPP interface, sessions on UUT and peer are UP, but “virtual-PPP1 is up, line protocol is down.”

  Conditions: For this symptom to occur, the virtual-ppp interface was previously deleted using the **no interface virtual-ppp** *n* command, and then reinstated using the **interface virtual-ppp** *n* command.

  Workaround: Be certain that the virtual-PPP interface has never been unconfigured using the **no interface virtual- ppp** *n* configuration command since the router was booted.

- CSCir00712

  Symptoms: When a LAC receives fragmented data traffic over an L2TP tunnel, the IP layer reassembles the packets and routes them over the wrong interface instead of processing them locally.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel. The symptom is release-independent.

  Workaround: There is no workaround.

- CSCsb24255

  Symptoms: A router may generate the following error message and a MALLOC failure may occur:

```
flex_dsprm_voice_connect: voice tdm connect failed
```

Conditions: This symptom is observed on a Cisco router that processes a large number of calls with a short call duration via an E1 PRI.

Workaround: There is no workaround.

- CSCse05777

  Symptoms: A router may reload unexpectedly when you configure more multilink interfaces than the maximum number that the router can support. The router should not reload but should generate an error message.

  Conditions: This symptom is observed on any Cisco router that imposes a limit on the number of multilink interfaces.

  Workaround: Do not exceed the maximum number of multilink interfaces.

- CSCse12198

  Symptoms: Individual B-channels on the primary T1 in the NFAS group sometimes go OOS for no reason.

  Conditions: This symptom is observed when connected to a Cisco PGW that is running Cisco IOS Release 9.3(2). The Cisco AS5400 is connected to the Cisco PGW that is running RLM in the Signaling/Nailed mode.

  Also, sometimes ISDN service goes OOS, and also channel states goes to 5 which is maintenance pending.

  Workaround: When this happens, put ISDN service can be put back in service manually for individual CIC, but channel state cannot manually be put back in service unless the whole serial interface is bounced. This cannot be done when there is other traffic on the other b-channels.

- CSCse34162

  Symptoms: A Cisco router hangs after 5 to 10 minutes of passing traffic over a dialer interface.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 12.4(8) with PPP Multilink configured on a dialer interface and traffic is passing.

  Workaround: There is no workaround. A reboot is required to recover.

- CSCse78652

  Symptoms: The queuing mode on multilink interfaces erroneously defaults to fair-queuing instead of FIFO, causing distributed Cisco Express Forwarding (dCEF) to fail.

  Conditions: This symptom is observed on a Cisco 7500 series and occurs for all multilink interfaces. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse81069

  Symptoms: Unconfiguring the **isdn service b_channel** command is not taking effect. The command is not removed from the running configuration.

  Conditions: This symptom occurs when configuring the **isdn service b_channel** command to a state other than the default value of 0 on the ISDN D channel.

  Workaround: To remove the command, shut down the T1/E1 controller first and then unconfigure the command under the D channel serial interface.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

Workaround: There is no workaround.

- CSCsg15642

  Symptoms: A PSTN Gateway unexpectedly restarts due to a lack of memory. Overtime memory utilization increases, and the **show processes memory sorted** command indicates that the ISDN process is allocating an increased amount of memory.

  Conditions: This leak occurs when a SETUP message with Display IE is received.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg40885

  Symptoms: A router crashes during Online Insertion and Removal (OIR) on MLP- PPP on a Cisco 7200 platform.

  Conditions: This symptom is observed on a Cisco 7200 router that is configured for MLP-PPP.

  Workaround: Shut the multilink interface before doing an OIR.

- CSCsg50202

  Symptoms: When BRI interface flaps rapidly, ISDN Layer 1 detects link down, but Layers 2 and 3 keep active state during the transition. This may cause the BRI interface to get stuck, where subsequent incoming/outgoing call is rejected.

  Conditions: The symptom may be observed when cable is pulled out and put back rapidly.

  Workaround: Issue the **clear interface** command or the **shutdown** command followed by the **no shutdown** command on the affected BRI interface.

Resolved Caveats—Cisco IOS Release 12.4(7c)

Cisco IOS Release 12.4(7c) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7c) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsd26248

  Symptoms: A router set up to do dot1x authentication without accounting setup may experience a memory leak in process RADIUS until the process consumes all free memory.

Conditions: This leak occurs on a router doing dot1x authentication without dot1x accounting configured and is sent attributes 24 (state) or 25 (class) from the Radius server.

Workaround: There is no workaround.

- CSCsd49317

  Symptoms: A crash occurs by processor memory corruption.

  Conditions: This symptom happens when configuring “no tacacs-server administration” and “tacacs-server administration” was not previously configured.

  Workaround: Do not configure “no tacacs-server administration.”

IP Routing Protocols

- CSCek14600

  Symptoms: A traceback has been seen on this release.

  Conditions: The symptom has been observed on Cisco IOS interim Release 12.4(04) T1fc2.

  Workaround: There is no workaround.

- CSCse29428

  Symptoms: A crash is seen with %ALIGN-1-FATAL after showing %SYS-2-CHUNKEXPANDFAIL and %SYS-2-MALLOCFAIL repeatedly.

  Conditions: This symptom is observed on a Cisco 3725 router that is running Cisco IOS Release 12.4(5a) with the c3725-advipservicesk9-mz image that is running IPSec VPN.

  Workaround: There is no workaround.

Miscellaneous

- CSCek45461

  Symptoms: Path confirmation fails for voice calls on a Cisco AS5850. One-way audio may occur with manual phones.

  Conditions: These symptoms are observed on a Cisco AS5850 that processes MGCP, H.323, and SIP calls.

  Workaround: There is no workaround.

- CSCek52778

  Symptoms: Dialer idle timer is not reset by interesting traffic on ISDN NON- MLPP, Async MLPPP, Async PBR user sessions.

  Conditions: This symptom is found on a Cisco AS5850 that is running Cisco IOS Release 12.4(7b). Problem may occur with involvement of virtual profiles.

  Workaround: There is no workaround.

- CSCin85894

  Symptoms: This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: A “%SYS-3-MGDTIMER” error message followed by a traceback may be generated at the “mgd_timer_complain_uninit” function when an extended ACL is configured with the same name as an active reflexive ACL.

Condition 1: This symptom is observed when the extended ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the extended ACL.

Workaround 1: Wait until the reflexive timer expires before you configure an extended ACL with same name as a reflexive ACL.

Symptom 2: A software-forced reload may occur when a standard ACL is configured with the same name as an active reflexive ACL.

Condition 2: This symptom is observed when the standard ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the standard ACL.

Workaround 2: Wait until the reflexive timer expires before you configure a standard ACL with same name as a reflexive ACL.

- CSCsb99936

  Symptoms: The **show ephone** command reveals a call is stuck in the SEIZE state instead of progressing to the correct state during a call.

  Conditions: This symptom has been observed when an H.323 call is placed from CME to a non-CME H.323 endpoint.

  Workaround: There is no workaround.

- CSCsc97398

  Symptoms: The user information Layer 1 protocol may be included in the outgoing bearer capability and may be set to either G711 u-law or G711 A-law. Some PBXs may refuse the call because of this mismatch in the bearer capability.

  Conditions: This symptom is observed when a call is made from H.323 to ISDN with unrestricted digital information bearer capability.

  Workaround: There is no workaround.

- CSCsd13419

  Symptoms: A Cisco 3700 series that functions as an RSVP agent may generate a Cisco IOS crash file in flash memory.

  Conditions: This symptom is observed in a topology that includes a Cisco CallManager that is configured for RSVP and two RSVP agents that function as transcoders, one of which is the affected Cisco 3700 series.

  Workaround: There is no workaround.

- CSCsd35389

  Symptoms: When a Cisco Unified CallManager Express (Cisco Unified CME) registers with a gatekeeper, all the ephone-dns are automatically registered. When an ephone-dn is deleted, it does not unregister with the gatekeeper. If you enter the **no gateway** command followed by the **gateway** command on the CME router to force it to unregister then reregister, the deleted ephone-dn will show up again.

  Conditions: This symptom is observed on a Cisco 3800 series router.

  Workaround: To permanently remove the ephone-dn reload the CME/gateway or enter the **shut** command followed by the **no shut** command on the gatekeeper.

- CSCsd37629

  Symptoms: Alignment errors and a bus error may occur on a Cisco platform that has the **ip inspect** command enabled.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 or Release 12.4T.

Workaround: Disable the **ip inspect** command.

- CSCsd66800

  Symptoms: A gateway-controlled T.38 fax relay between an MGCP gateway and another gateway may be disconnected unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that is configured for Voice xGCP.

  Workaround: There is no workaround.

- CSCsd88768

  Symptoms: With PPP multilink configured on serial links on PA-MCX-8TE1,the following error message may be seen:

  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0

  Conditions: With PPP multilink configured on serial links on PA-MCX-8TE1 and when traffic is flowing, the following error message may be seen:

  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0

  Workaround: There is no workaround.

- CSCse05642

  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

- CSCse55652

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

  Conditions: This symptom is observed on a distributed router such as a Cisco AS5850 or Cisco 7500 series that runs Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCse63494

  Symptoms: A router that is configured for Real-Time Protocol (RTP) may generate CPUHOG events and a traceback similar to the following:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  ```

```
(951/33),process = VOIP_RTCP.
-Traceback= 0x60EA5A78 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
```

Alternatively, the router may unexpectedly reload and generate the following error message and traceback:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = VOIP_RTCP. -
Traceback= 0x60EA5A58 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
%Software-forced reload
Preparing to dump core...
```

Conditions: This symptom is observed on a Cisco router that receives a badly formatted RTP Control Protocol (RTCP) packet.

Workaround: There is no workaround.

Further Problem Description: Typically, the badly formatted RTCP packet is produced by a device that does not conform to the RFC 3550 standard.

- 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

- CSCse68355

  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

- CSCse85329

  Symptoms: When you re-insert a PA-MC-8TE1+ port adapter in the same slot of a Cisco 7200 series via an OIR, the serial interface may enter the Down/Down state. When you enter the **shutdown** command followed by the **no shutdown** command on the T1 or E1 controller, the serial interface may transition to the Up/Down state, still preventing traffic from passing.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(7) or a later release.

  Workaround: Reload the router.

- CSCse89105

  Symptoms: RADIUS packets may be dropped or extra memory may be allocated when RADIUS packets are sent.

  Conditions: These symptoms are observed on a Cisco platform that is configured for SSG when a RADIUS packet with a length of more than 1024 bytes is sent.

  Workaround: There is no workaround.

- 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

Wide-Area Networking

- CSCek28604

  Symptoms: A Cisco device may reload (“System returned to ROM”) unexpectedly due to a memory leak in the ISDN L2 process.

  Conditions: This symptom is observed on a Cisco device that functions in a call manager-backhaul configuration after running under stress for about 24 hours.

  The output of the **show processes memory**, collected in regular intervals shows a memory leak in the ISDN L2 process. The amount of memory that is held by the ISDN L2 process will be very large and growing.

  Workaround: Enter the **isdn k 1** command on all backhauled serial interfaces.

- CSCse79994

  Symptoms: BRI Layer 2 remains in the ESTABLISH_AWAITING_TEI state instead of entering the MULTIPLE_FRAME_ESTABLISHED state.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

- CSCsf03251

  Symptoms: Primary and backup NFAS interfaces may transition from WAIT to OOS even after receiving “in-service” message from the PSTN.

  Conditions: This symptom is observed on a Cisco AS5400XM that is running several Cisco IOS 12.4 mainline and 12.4T releases.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7b)

Cisco IOS Release 12.4(7b) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCea36491

  Symptoms: When entering the routers configuration mode or like to see the running configuration, the session could hang. When these symptoms occur, interfaces may enter the wedged state with Simple Network Management Protocol (SNMP) traffic.

  Conditions: Sending Simple Network Management Protocol (SNMP) configuration traps are enabled. Although the problem is found on ATM and Packet over SONET (POS) interfaces, this behavior is independent of the interface and Cisco IOS based platform.

  Workaround: Disable Simple Network Management Protocol (SNMP) configuration traps by entering the CLI **no snmp-server enable traps config** global configuration command.

- CSCek33076

  Symptoms: Progress code may be reported as LCP open for IPCP failed calls.

  Condition: This condition was observed on a Cisco AS5400 that is running Cisco IOS Release 12.4(3a).

  Workaround: There is no workaround.

- CSCek40060

  Symptoms: RADIUS server authentication may not function for dialup and PPP clients.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) and that has the **radius-server retry method round-robin** command enabled.

  Workaround: Disable the **radius-server retry method round-robin** command. Note that the symptom does not occur in Release 12.3 or Release 12.3T.

- CSCin99788

  Symptoms: %AAA-3-ACCT_LOW_MEM_TRASH error message spewed when run into low memory, and AAA related data could be leaked after hitting this condition.

  Conditions: The likely trigger is an interface flap with a huge number of sessions going down simultaneously generating enormous accounting-stop records. A sluggish/unreachable AAA server IO memory would be held for a long time retrying to send the accounting records.

  Workaround: There is no workaround.

- CSCsb71584

  Symptoms: A spurious memory access is generated in the “aaa_string_vsa_prefix_to_protocol” function.

  Conditions: This symptom is observed on a Cisco platform that is configured for Network Admission Control (NAC).

  Workaround: There is no workaround.

- CSCsc97727

  Symptoms: An access point may crash when you add or remove TACACS servers via the CLI.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(7)JA1 or Release 12.3(7)JA2 and that has the **aaa accounting commands** *level* **default** *list-name* **group** *groupname command enabled. The symptom may also occur in other releases.*

  Workaround: Disable the **aaa accounting commands** *level* **default** *list-name* **group** *groupname command.*

  Alternate Workaround: Use RADIUS instead of TACACS.

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

  Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

  Workaround: There is no workaround.

- CSCse09594

  Symptoms: A router crashes during the AAA authentication process for interfaces that are configured for PPP.

  Conditions: This symptom is observed on a Cisco router when the memory is exhausted. For example, the symptom may occur on a router that attempts to bring up more PPP sessions while its memory usage is already higher than 99 percent of the capacity because of existing configuration and sessions.

  Workaround: There is no workaround.

- CSCse49728

  Symptoms: SNMPv3 informs are not sent out after a device reload.

  Conditions: This symptom is observed when SNMPv3 informs have been configured, and the device is reloaded.

  Workaround: Re-enter any of the **snmp-server host** commands.

Interfaces and Bridging

- CSCek27833

  Symptoms: Pings with a datagram size of 1485 and above are not going across the bridge.

  Conditions: This symptom is observed on a serial interface configured for PPP and part of the bridge group on a Cisco router.

  Workaround: Increase the MTU size on the interfaces. For example, configure an MTU of 1524.

- CSCsc66187

  Symptoms: Error messages such as the following one may be generated on a Cisco 7500 series or Cisco 7600 series:

  ```
  %CWPA-3-IPCALLOCFAIL: Failed to allocate IPC buffer for loveletter data
  ```

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured with a 1-port Packet-over-SONNET OC-3c/STM-1 multimode port adapter (PA-POS-OC3MM) when you enter the **no shutdown** interface configuration command on the interface.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed84633

  Symptoms: When you enter the **distribute-list** command

  under the **address-family ipv4** command, the **distribute-list** command does not take effect.

  Conditions: This symptom is platform- and release-independent.

  Workaround: There is no workaround.

- CSCek29860

  Symptoms: A Cisco router may experience a software-forced crash.

  Conditions: This symptom is observed on a Cisco router that is configured for secure NAT (SNAT), NAT Stateful Failover, and HSRP.

  Workaround: There is no workaround.

- CSCek32244

  Symptoms: Not all classful networks are locally generated in the BGP table.

  Conditions: This symptom is observed on a Cisco router that has the **auto-summary** command enabled and occurs when classful networks are provided before the routes are made available in the routing table.

  Workaround: There is no workaround.

- CSCse04220

  Symptoms: The BGP table version remains stuck at 1 following the issue of the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. Issuing the **clear bgp ipv4 uni *** or **clear bgp ipv6 uni *** commands may also result in a crash.

  Conditions: This symptom occurs when issuing the **clear bgp ipv4 uni *** or **clear bgp ipv6 uni *** commands.

Workaround: Using the **clear ip bgp *** command clears the sessions, and the BGP table is purged. The **clear ip bgp *** command will also avoid crashing the router.

- CSCuk58462

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- CSCuk60585

  Symptoms: A router that is configured for redistribution into ISO-IGRP may crash.

  Conditions: This symptom is observed when the configuration is NVgened.

  Workaround: There is no workaround.

Miscellaneous

- CSCef29090

  Symptoms: The throughput for TCPClear sessions on a Cisco AS5850 may not be as expected and there may be a slow response time.

  Conditions: This symptom is observed on a Cisco AS5850 with TCPclear sessions.

  Workaround: There is no workaround.

- CSCei84353

  Symptoms: A router crashes when you remove an Embedded Event Manager (EEM) applet.

  Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S. This symptom occurs under the rare occasion that the EEM applet is removed while EEM is attempting to trigger the applet for execution.

  Workaround: Perform the following three steps:

  1) Before you remove the EEM applet, disable EEM applet scheduling by entering the **event manager scheduler applet suspend** command.

  2) Remove the applet.

  3) After you have removed the applet, re-enable EEM applet scheduling by entering the **no event manager scheduler applet suspend** command.

- CSCej29710

  Symptoms: Unable to send EEM type system SNMP trap notifications.

  Conditions: This symptom occurs when users want to send EEM SNMP system type trap notifications upon triggering of a policy.

Workaround: In EEM applet mode if a user desires an SNMP notification upon event trigger, they should specify it as an action by using the **action snmp-trap** command. In EEM TCL policies, use the **action_snmp_trap** TCL command.

- CSCek24468

  Symptoms: Dangling bearer channels or voice DSP channels may occur.

  Conditions: This symptom is observed under heavy stress with short duration calls on a Cisco platform such as a Cisco AS5400 or Cisco AS5850 that functions as a gateway.

  Workaround: There are no workaround.

- CSCek26155

  Symptoms: A recursive pattern scan loop can occur when the Embedded Event Manager (EEM) CLI ED attempts to scan for patterns provided by action CLI commands.

  Conditions: This issue occurs when an applet contains a CLI event that is scanning for a pattern that is given as a CLI command in one of its actions. See the following example:

  ```
  event manager applet one event CLI pattern "show version" sync yes action 1 CLI command
  "show version"
  ```

  In this example the action being performed causes the event to trigger in a loop.

  Workaround: Do not use an action CLI command containing a pattern that matches the CLI event pattern.

- CSCek34049

  Symptoms: A Cisco AS5850 that is configured for RPR+ may be unable to process more than 1990 MGCP voice calls. With more than 1990 MGCP voice calls, any of the following symptoms may occur:

  - Many DSP may time-out.
  - Active calls may hang.
  - Spurious memory accesses and tracebacks may be generated.
  - Incoming calls may be dropped.
  - NextPort SPE ports may be stuck in the "a" state.

  Conditions: These symptoms are observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(3d) or Release 12.4(7a).

  Workaround: There is no workaround. A Cisco AS5850 that is used to its full capacity (4 CT3 worth of MGCP calls) may not scale beyond 1990 calls. When the symptoms have occurred, reload the Cisco AS5850.

- 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

- CSCek37686

  Symptoms: A Cisco AS5350 may reload because of a bus error (SIG=10).

  Conditions: This symptom is observed when SNMP is configured and when SNMP queries are made into the Cisco AS5350.

  Workaround: Disable SNMP or stop polling the router.

- CSCek38136

  Symptoms: When you deploy VoIP using PVDM2 / 5510 DSP modules, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with 5510 DSP modules. The symptom does not occur with 549 DSP modules.

  Workaround: There is no workaround.

- CSCek42816

  Symptoms: A voice gateway reloads under bulk calls.

  Conditions: This symptom occurs when a voice gateway that is running VXML applications streaming voice gets prompts from the HTTP server.

  Workaround: Configure the following on the router:

  ivr prompt streamed none

- CSCek43642

  Symptoms: When you try to remove an Embedded Event Manager (EEM) policy that has event criteria specified via the **event_register_appl** Tcl command extension, the attempt fails.

  Conditions: This symptom is observed when two or more Embedded Event Manager policies are configured and when only one of these policies has event criteria specified via the **event_register_appl** Tcl command extension.

  Workaround: There is no workaround.

- CSCek47283

  Symptoms: The router cannot be reloaded using the **reload** command. The following message is displayed when trying to reload the router:

  ```
  The startup configuration is currently being updated. Try again.
  ```

  Conditions: This symptom occurs in some rare conditions. It may be triggered after the “Invalid pointer value in private configuration structure” message is displayed (as seen in CSCin98933). This symptom is observed in Cisco IOS Interim Releases 012.003(019.007), 012.004(006.005), 12.4(06.05)T, and its later releases.

  Workaround: There is no workaround.

- CSCsb95563

  Symptoms: On rare occasions, Embedded Event Manager (EEM) may cause a crash when unregistering an EEM policy.

  Conditions: This crash is seen on Cisco Catalyst 6000 images. The crash occurs when unregistering EEM policy.

  Workaround: There is no workaround.

- CSCsc12255

  Symptoms: When you deploy VoIP on an NM-HDV2 network module that is configured with a PVDM2-64 module, a hissing sound may be heard before the ringback tone starts on the calling side.

Conditions: This symptom is observed only with an NM-HDV2 network module. Note that the symptom does not occur with an NM-HDV network module.

Workaround: There is no workaround.

- CSCsc18707

  Symptoms: No error message is printed out when running an Embedded Event Manager (EEM) policy that is not registered with the none event detector.

  Conditions: This symptom occurs when executing **event manager run** *policy name* or **action label policy** *policy name* command, but the policy is not registered with the none event detector.

  Workaround: There is no workaround.

- CSCsc70644

  Symptoms: A CLI session may become stuck during the configuration of QoS.

  Conditions: This symptom is observed on a Cisco router after you have entered the **show policy-map interface** command.

  Workaround: There is no workaround.

- CSCsc95234

  Symptoms: When the **stcapp** global configuration command is enabled, the command is not accepted and the following error messages are generated:

  ```
  STCAPP: Internal error: Unable to create codec list... exiting stcapp shutdown
  initiated... waiting for calls to clear. stcapp shutdown complete.
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(6.3) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCsd08862

  Symptoms: A router may crash because of a bus error when you enter the **show interface** command for a virtual-access interface or subinterface.

  Conditions: This symptom is observed when you enter the **show interface** command while a session that is associated with the virtual-access interface or subinterface is being cleared.

  Workaround: There is no workaround.

- CSCsd11811

  Symptoms: A Cisco 1760 router that is running Cisco IOS Interim Release 12.4(6.7) may reload due to a software-forced crash.

  Conditions: The trigger is due to improper packet cleanup when the buffer allocation fails under high CPU load.

  Workaround: There is no workaround.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that is running Cisco IOS Release 12.4(3)B. The router has services 81, 82 and 90 configured. The only service having a problem is 90. The packet traces indicate that the router is sometimes responding to Here_I_Am messages from the cache with I_See_You messages containing an incorrect destination IP address. This leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(3)B.

  Workaround: There is no workaround.

- CSCsd41070

  Symptoms: Calls are dropped because of a backhaul link failure during a switchover of a Cisco PGW 2200 Softswitch.

  Conditions: This symptom is observed on a redundant Cisco PGW 2200 Softswitch system that is connected to a Cisco AS5850 and that is configured for MGCP-controlled PRI backhaul. Calls drop after the switchover of the Cisco PGW 2200 Softswitch because there is a disconnect between the Layer 2 and the D channel.

  Workaround: There is no workaround.

- CSCsd47734

  Symptoms: A memory leak may occur when you run an EEM Tcl policy.

  Conditions: This symptom is platform- and release-independent.

  Workaround: There is no workaround.

- CSCsd61780

  Symptoms: A router crashes because of errors from checkheaps.

  Conditions: This symptom is observed when hundreds of CLI commands are entered in virtual-template mode.

  Workaround: There is no workaround.

- CSCsd73526

  Symptoms: When using CSS in a design for CVP, the Cisco IOS Voice Browser cannot play the media file after upgrading the Cisco IOS from Cisco IOS Release 12.3(3a) to Release 12.4(3b). CSS does send the HTTP Redirect pointing to CVP, but the gateway does nothing with it.

  Conditions: This symptom has been observed when the following are present:

  - AS5400HPX
  - Cisco IOS Release 12.4(3b)
  - CVP 3.1 SR1 - ICM 6.0
  - CallManager 4.1(3) SR 2

  Workaround: Bypass CSS, and point the VXML application directly to CVP.

- CSCsd73749

  Symptoms: Traffic that is processed by PVCs with a small bandwidth on an NM-1M-OC3-POM network module may encounter large latencies and may be dropped from the output queue.

  Conditions: This symptom is observed on a Cisco router that is configured with an NM-1A-OC3-POM network module when the PVCs have a small bandwidth that is less than 10 Mbps.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat provides the following solution:

  On ATM line cards, the SAR mechanism has a queue for each PVC. Two thresholds are associated with each PVC queue: the high watermark and low watermark. The high watermark defines the number of cells that the queue can hold.

  The watermark values are used to apply a flow control mechanism between the host and the SAR on the NM-1A-OC3POM network module. When cells start backing up in the SAR, the SAR sends a notification to the host as soon as the queue inside the SAR builds up to a high watermark. At this point, the VC is marked as throttled and packets start backing up in the Cisco IOS software hold

queues. At the same time, the SAR is draining out the packets. When the SAR reaches the low watermark, another notification is sent to the host. The VC is marked as "Open" and traffic to the VC resumes. The problem is caused by the low values that are configured for the high and low watermarks on the SAR.

To configure watermark values that are suitable for your applications, use the **queue-depth** command, which is available in a Cisco IOS software image that integrates the fix for caveat CSCsd73749.

The command syntax and usage are explained below:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int atm 1/0
Router(config-if)#pvc 1/1
Router(config-if-atm-vc)#queue-depth ?
  <1-65535>  queue depth high watermark, in cells

Router(config-if-atm-vc)#queue-depth 200 ?
  <1-200>  queue depth low watermark, in cells

Router(config-if-atm-vc)#queue-depth 200 100 ?
  <cr>

Router(config-if-atm-vc)#queue-depth 200 100
Router(config-if-atm-vc)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Note that the default values of watermarks are not changed in a Cisco IOS software image that integrates the fix for caveat CSCsd73740.

Guidelines for configuring the watermarks are as follows:

A high watermark translates into larger queue build-up inside the SAR, affecting the latency of LLQ-type traffic. A low watermark translates into the use of the traffic shaping mechanism within the SAR. If a low watermark is too low, the SAR may drain its queue entirely, causing a breakage of traffic shaping.

In general, if you need to change the watermark values, follow these guidelines:

- For better latency, decrease the high watermark value.
- For a higher number of cells in the queue or for better TCP performance, increase the high watermark value.
- Do not configure the low watermark value to be equal to the high watermark value because this defeats the purpose of the flow control mechanism.
- Even though the **queue-depth** command allows a high watermark value up to 65535, we do not recommended that you configure such a high watermark value. A high watermark value translates into queues within the SAR. How high the value of the high watermark can be is defined by the SAR memory. For example, with 1024 VCs, when the high watermark is configured above 400 cells, the SAR may run out of memory, causing packet drops to occur.

  - Detailed guidelines about high and low watermark values will be provided in a separate document. As a rough guideline, default values of high and low watermarks for PVCs with a bandwidth of less than 1 Mbps are 50 and 10. The symptom may occur with these values. However, when you multiply these values by a factor of 4 via the **queue-depth** command such that the new values are 200 and 40, the symptom no longer occurs.

- CSCsd76444

  Symptoms: There is an unexpected reload of a Cisco router that is running PRE experiencing Signal 0 reload with no stack contents.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running PRE.

  Workaround: There is no workaround.

- CSCsd79558

  Symptoms: When tunnel protection is configured on a tunnel interface, an IPSec session may fail to come up.

  Conditions: This symptom is observed when the **tunnel vrf** *vrf-name* command is changed on the tunnel interface.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove and re-add the tunnel interface.

- CSCsd99763

  Symptoms: A Cisco 7200 series router reloads unexpectedly while configuring BGP access list.

  Conditions: This symptom is observed on a Cisco 7206VXR (NPE-G1) processor (revision A). The following commands serve as an example that causes router to reload unexpectedly:

```
config t
router bgp 100
neighbor EXTERNAL route-map MAP3 out
address-family ipv4 multicast
neighbor EXTERNAL route-map MAP3 out
!
ip as-path access-list 1 deny ^$
ip as-path access-list 2 permit ^(700)+(_1123)|_2374$|^(_700)+(_2374)+
(_1123)+$
ip as-path access-list 3 permit _3400_
ip as-path access-list 4 permit ^(700)+(_3400)|_1123$|^700$|_23\[0-9\]$
!
route-map MAP3 permit 10
match as-path 1
!
route-map MAP3 deny 20
match as-path 2
!
route-map MAP3 permit 30
match as-path 3
!
route-map MAP3 permit 40
```

```
match as-path 4
set metric 300
end
```

Workaround: There is no workaround.

- CSCse01847

  Symptoms: When agentless hosts are allowed network access, a loss of connectivity may occur during reauthentication.

  Conditions: This symptom is observed when the host does not have a Cisco Trust Agent (CTA) configured.

  Workaround: There is no workaround.

  Further Problem Description: When an agentless host is authorized for network access, a dynamic access policy is applied for the host. This access policy is removed at the beginning of the reauthentication process, and re-applied at the end of reauthentication process. During the reauthentication process, no access policy is applied for the host. This situation may cause a disruption to network access.

- CSCse15025

  Symptoms: An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

  When this problem occurs, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

  Because this issue impacts the signaling channels, it has been seen that calls either will not connect at all through impacted ports or in some cases when multiple simultaneous calls are present on adjacent voice ports/timeslots, the call may connect momentarily before being disconnected.

  If a problem occurs only on a single voice port, there is another problem, not this caveat (CSCse15025). PRI/BRI calls are not affected because PRI/BRI does not utilize the DSP for signaling purposes.

  When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port- number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41, and 42 is presented and some of the registers show double- octet information. See the example output (2) below.

  When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** *port- number* **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

  Further Problem Description: The changes in CSCse15025 includes changes in CSCsc11833 and CScsd90851. These changes have been shown to help mitigate this problem in the majority of cases.

There is a further detection and reset mechanism in CSCse15025 that will recover the DSP which is in this state. This mechanism will trigger immediately if the impacted voice port is an analog FXO port. For other voice ports, a delay in the detection will be present and it is possible to see the symptom of this problem before the recovery code triggers.

Note that the reset mechanism will cause any active calls utilizing the DSP in question to be dropped.

It is recommended if running with modules which can be impacted by this issue to upgrade to a release of software which contains the changes in CSCse15025. If the DSP is reset and the below output is seen, contact the TAC for further assistance. Note that this output is sent at debug level and it is recommended to enable either syslog or logging buffered on the gateway.

Logging buffered on the gateway is enabled through the global command **logging buffered 50000 debug** as an example to set the logging buffered to use 50K bytes of processor memory for logging. The output of the log can be seen with the exec command **show log.**

Example output when detection and recovery code on gateway triggers:

```
*May 31 14:30:43.343: TDM pointers: 0100 0100 0115 0115. Deltas: 0001 0000.

*May 31 14:30:43.347: Received alarm indication from dsp(0/1)
0030 0000 0080 0000 0013 4100 2E2E 2F2E 2E2F 6D6F 6475 6C65 732F 7363 6865
6475 6C65 2F64 6562 7567 2E63 2833 3634 2900
*May 31 14:30:43.347: ../../modules/schedule/debug.c(364)

*May 31 14:30:43.347: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to Administrative Shutdown
*May 31 14:30:43.647: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to Administrative Shutdown
*May 31 14:30:43.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to Administrative Shutdown
*May 31 14:30:44.247: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to Administrative Shutdown

*May 31 14:30:48.147: Crash dump CLI may not be configured, not able to get
crash info, slot 0, dsp 1
*May 31 14:30:48.147: DSPDUMP - Recover slot 0 dsp 1
*May 31 14:30:48.147: DSPDUMP - ka sent 0, ka_cnt 51193, skip_ka 103079
*May 31 14:30:50.579: %DSPRM-5-UPDOWN: DSP 1 in slot 0, changed state to up
*May 31 14:30:50.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to up
*May 31 14:30:51.219: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to up
*May 31 14:30:51.371: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to up
*May 31 14:30:51.523: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to up
----
```

Following are command output examples:

3. Following is an example of normal output for FXO and EVM FXS ports.

For FXO ports, the value is usually 0x01 but for EVM FXS the value can be different. When you run the above-mentioned command, the expected output is that a single octet is displayed and only for register 39. (This command does not work for VIC-4FXS and VIC2-xFXS modules).

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#

Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x01
```

4. Following is an example of output for FXO and EVM FXS ports that indicates that the symptom has occurred. Note that the exact output for the register values is different, but when the symptom occurs, different lines with information are displayed as shown below:

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#

Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF
```

5. Following is an example of normal output for FXS and analog E&M modules. The values that are listed in a normal case may be different, but only four registers of a single octet should be displayed.

```
Values read from PEB2465 Codec connected to DSP 02 (channel 0):
------------------------------------------------------------
Extended Register Values (XR4..XR1) = 00, CC, 50, 11
```

4) Following is an example of output for FXS and analog E&M modules that indicates that the symptom has occurred.

```
Values read from PEB2x65 Codec connected to DSP 0, channel 1:
------------------------------------------------------------
Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCse34097

  Symptoms: When a voice call is made to one of the busy channels of BRI/PRI port, the call gets rejected and then another call is made to the available port. The call gets connected, and the user hears an annoying hissing sound.

  Conditions: The procedure to recreate this scenario is the following:

  ```
  Phone a & b ---OGW --VoIP --TGW(2611) --BRI/PRI --PBX -- phone c & d
  ```

```
Phone a calls phone c;
Phone b calls phone c;
Phone b calls phone d;

Phone d picks up and hears a hissing noise.
```

Workaround: There is no workaround.

- CSCse45425

  Symptoms: VAM2 resets with the message “Free Pool stuck”. The IPSec SAs are transferred to software crypto. This causes 100% CPU.

  Conditions: The decrypted packet total size does not match the total length in its IP header.

  Workaround: There is no workaround for the VAM2 reset. However, during the VAM2 recovery, disable software encryption by issuing the **no crypto engine software ipsec** command to force encryption back to hardware.

- CSCse55557

  Symptoms: This symptom is seen when the **show policy-map control-map** command is issued in the router CLI when there are no control- plane service policies configured.

  Conditions: This problem will occur for any attempt to view service-policy information when there is no such service policy.

  Workaround: There is no workaround.

- CSCse56660

  Symptoms: Inbound calls to FXO ports on Cisco IOS VoIP gateways connect, but audio is not present.

  Conditions: With **caller-id enable** configured on FXO ports, the call will connect, but no audio is heard. When this occurs, the following error message can be seen at debug level:

  ```
  Jun 20 01:41:15.855: mbrd_e1t1_vic_connect: setup failed
  Jun 20 01:41:15.855: flex_dsprm_tdm_xconn: voice-port(0/0/1), dsp_channel
  (/0/2/0)
  ```

  Workaround: Disable caller id on the voice-port.

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

  Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third party system.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCeh64479

  Symptoms: A router reloads unexpectedly when an apparent Layer Two Forwarding (L2F) packet is received.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Virtual Private Dialup Network (VPDN). However, the symptom is not platform-specific.

Workaround: There is no workaround.

- CSCej20215

  Symptoms: Calls could not be placed once the router was upgraded from Cisco IOS Release 12.3(14)T to Cisco IOS Release 12.4(3).

  Conditions: This symptom has been observed with Cisco IOS 12.4(3) and placing calls using the E1 EuroISDN link.

  Workaround: Install Cisco IOS Release 12.3(14)T.

- CSCek31660

  Symptoms: For VPDN sessions that are established with a LAC, the RADIUS progress code in the Stop record may be different from the RADIUS progress code in the Start record.

  Condition: This symptom is observed on a Cisco platform such as a Cisco AS5400 that runs Cisco IOS Release 12.4.(3a) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCek40618

  Symptoms: A Cisco 7200 series router may crash by address error (load or instruction fetch) exception, CPU signal 10, during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCsd19867

  Symptoms: BRI interfaces does not come up when you reload a router. You must enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected BRI interfaces to bring them up.

  Conditions: This symptom is observed when you enter the **no isdn spoofing** command and reload the router.

  Workaround: Disable the **no isdn spoofing** command.

- CSCsd47777

  Symptoms: Any PPP session that runs on a subinterface may crash.

  Conditions: This symptom is observed with PPPoA, PPPoE, or VPDN sessions on a subinterface.

  Workaround: Enter the **no virtual-template subinterface** command globally.

- CSCsd51082

  Symptoms: An ISDN Layer 2 may not become active after a failure.

  Conditions: This symptom is observed when ISDN backhaul is configured.

  Workaround: There is no workaround.

- CSCsd71134

  Symptoms: The spurious memory access pointing to ppp_up_simple may be seen on an RPM-XF that is running Cisco IOS 12.4T.

  Conditions: This symptom occurs rarely.

  Workaround: There is no workaround.

- CSCsd79611

  Symptoms: L2TP sessions are not established when multihop is configured.

  Conditions: This symptom is observed when SGBP is configured in a multihop environment. The L2TP sessions fail to be established because the source IP address is marked as down.

  Workaround: There is no workaround.

- CSCsd81350

  Symptoms: When asynchronous serial interfaces are used as member links in multilink PPP bundles, the router may crash due to memory corruption.

  Conditions: This problem can occur under conditions where multilink fragmentation is done, and where the bundle includes at least one member link that is an asynchronous interface.

  Workaround: Disable fragmentation on the bundle interface for any bundle that may include asynchronous links as members. Alternatively, if the use of multilink is not a requirement, disable multilink on the asynchronous interfaces.

- CSCse16539

  Symptoms: VPDN loadbalancing incorrectly biases to one LNS (IP address) instead of sharing the session load between the different LNSs after LNS return from the busy list.

  Conditions: This occurs when multiple LNSs are configured for one vpdn-group and are unreachable. They are moved to the busy list. Once the LNSs become reachable again, this problem occurs.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7a)

Cisco IOS Release 12.4(7a) is a rebuild release for Cisco IOS Release 12.4(7). The caveats in this section are resolved in Cisco IOS Release 12.4(7a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsb30875

  Symptoms: Active eRSC on a Cisco AS5850 gateway could hang after RPR+ failover, if the **aaa accounting system** command is configured.

  Conditions: The symptom has been observed under the following conditions:

  1. RPR+ failover occurred.
  2. Console connection window closed & reopened to the newly active eRSC after failover.

  Workaround: There are two workarounds.

  1. The eRSC hang will not happen if no attempt is made to close and reopen the console session with newly active eRSC after failover.
  2. Remove the **aaa accounting system** command from the configuration.

- CSCsb43767

  Symptoms: Radius packets being sent have the incorrect value for attribute 5 (Nas-Port). The Async interface-related information is needed in the Cisco-Nas- Port attribute.

Conditions: This symptom has been observed on the Cisco-Nas-Port attribute on a radius server.

Workaround: There is no workaround.

- CSCsd10306

  Symptoms: IP SLA packets are dropped in the network. They may also cause a buffer leak on some Cisco routers. Frequency of the problem is very low, less then 1%.

  Conditions: This symptom is observed on IP SLA packets that have an MPLS label applied on the source router.

  Workaround: There is no workaround.

  Further Problem Description: The IP SLA packets in question have a corrupted IP header.

IP Routing Protocols

- CSCef03271

  Symptoms: BGP fails to advertise routes to peers that were learned from another source.

  Conditions: This symptom occurs when the neighbor clears the BGP session.

  Workaround: Clear the session using a soft reset and enter the **clear ip bgp** *neighbor-address* **soft in** command.

- CSCeg39601

  Symptoms: The IPv6 multicast RP encapsulation tunnel remains down.

  Conditions: This symptom occurs on the configuration of the **ipv6 pim rp-address** command. The resulting encapsulation tunnel is created but remains always in down state.

  Workaround: There is no workaround.

- CSCek33991

  Symptoms: A router may reset unexpectedly when it is in the midst of output of the results of the **show interface dampening** command, and the interface is deleted from another vty connection.

  Conditions: This symptom can be encountered if concurrent connections are opened to a router, and the **show interface dampening** command is issued while interface(s) are deleted.

  Workaround: Ensure interfaces with **dampening** configured are not deleted while the **show interface dampening** command can be possibly issued on another vty.

- CSCsc72090

  Symptoms: A router that is configured for EIGRP may fragment packets if the MTU on the interface is set to a value that is lower than 1500 bytes. This situation may cause additional overhead for the receiving router that must reassemble the packets.

  Conditions: This symptom is observed on a Cisco router that transmits packets that are larger than the MTU on the interface and occurs because EIGRP does not automatically adjust to the value of the MTU on the interface.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat prevents EIGRP from sending packets that are larger than the MTU of the interface MTU in order to prevent fragmentation.

- CSCsc78813

  Symptoms: While using NAT in an overlapping network configuration, the IP address inside a DNS reply payload from the nameserver is not translated at the NAT router.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(18) and that has the **ip nat outside source** command enabled. The symptom could also occur in Release 12.4 or Release 12.4T.

Workaround: There is no workaround.

- CSCsc94867

  Symptoms: A traceback is generated in the log after NAT entries are created on a PE router that is configured for NAT and that has a static NVI.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(5.12) or interim Release 12.4(5.13)T2.

  Workaround: There is no workaround.

- CSCsc98828

  Symptoms: PIM becomes disabled on an output interface, preventing packets from being sent, and causing the SR flag to be set after 60 seconds on the router that functions as the first hop.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 PIM.

  Workaround: There is no workaround.

- CSCsd27388

  Symptoms: A ping from a source to a destination fails because of an encapsulation failure.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for NAT and that has the **ip nat inside source static** command enabled on a VRF.

  Workaround: There is no workaround.

Miscellaneous

- CSCee72997

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCeh60551

  Symptoms: Certain malformed client certificates may cause an AP running 12.3.2.JA2 or 12.3.4.JA to crash when EAP-TLS is used.

  Workaround: Issue a new client certificate.

- CSCek26158

  Symptoms: A memory leak may occur on a router that is configured for Embedded Event Manager (EEM).

  Conditions: This symptom is observed when EEM Tcl policies are registered to run on the router.

  Workaround: There is no workaround.

- 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

- CSCek27181

  Symptoms: Cisco Land Mobile Radio (LMR) VoIP may not function.

  Conditions: This symptom is observed when multicast if configured.

  Workaround: There is no workaround.

- CSCek29792

  Symptoms: A router that is configured for voice may crash because of a bus error and an error message similar to the following may be generated:

  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x400BA2B8

  Conditions: This symptom is observed when all the following conditions occur:

  1) Redirection is triggered by a feature other than Call Forward Busy or Call Forward All.

  2) The calling party such as a user with an FXS phone does not support redirection.

  3) If a TCL script is used, the rerouteMode is set to REDIRECT_ROTARY.

  4) The rerouteNumber is an invalid E.164 number or URL.

  Workaround: There is no workaround.

- CSCek30748

  Symptoms: A router reloads when you enter the **tunnel protection ipsec profile vpnprof** command.

  Conditions: The symptom can be observed on a Cisco 7200 series but may be platform-independent.

  Workaround: There is no workaround.

- CSCek33253

  Symptoms: NextPort modems that function in a T1 CAS signaling configuration do not dial all the DTMF digits successfully.

  Conditions: This symptom is observed when you enter valid DTMF digits such as # and * in dial a string.

  Workaround: Use MICA modems instead of NextPort modems.

  Alternate Workaround: Use ISDN PRI T1 instead of T1 CAS signaling.

- CSCek34617

  Symptoms: A spurious memory access is generated when the router is booting up after a power-cycle or reload.

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3700 series, and Cisco 3800 series that have a virtual asynchronous auxiliary interface configured.

  Workaround: Remove the **interface async1** command from the running configuration and reload the router.

- CSCin98933

  Symptoms: A Cisco Router displays the following error message when issuing the **write memory** or **copy running-config startup-config** or "copy <file1> nvram:startup-config" or while booting up the image itself:

  NV: Invalid Pointer value(6357F3CC) in private configuration structure

  Conditions: This symptom is observed under the following conditions:

  1. The router is running Cisco IOS Interim Releases 12.4(06.05), 12.4(06.05) T, or later releases. That is, the Cisco IOS image should have the fix for CSCsc61630.
  2. This error message will be hit when the NVRAM is corrupted. This kind of NVRAM corruption occurs in rare conditions.
  3. This is seen only on a few platforms like the Cisco 3725, Cisco 3745, Cisco 3825, Cisco 3845, Cisco 2600, Cisco 2800, Cisco RPM, Cisco RPMXF cards, and Cisco AS5400. This bug is not seen on the Cisco 7200 and Cisco RSP routers.

  Workaround: See the following:

  1. You can issue the **erase nvram:** or **write erase** command to initialize the geometry of NVRAM. Then issue the **write memory** command to copy the running-configuration to startup-configuration. This solution can be taken only as a quick, temporary solution. For permanent solution, please see "Further Problem Description."
  2. It is always better to have a backup copy of the startup-configuration in some other storage device.
  3. The current running-configuration can be stored in some storage device other than NVRAM by issuing the **copy running-config** *storage device other than NVRAM*:*configuration file name* command.

  Further Problem Description: This problem may be seen after upgrading to Cisco IOS Interim Release 12.4(006.005), 12.4(06.05)T or later releases.

  Explanation: There is a stale, unerased private-configuration pointer in NVRAM, other than the original private-configuration pointer. Since this pointer is an invalid one, the Cisco IOS detects this corruption and reports this error. This error message will be hit only in rare circumstances.

  It is recommended that once the Cisco IOS image is upgraded to the aforementioned versions, take the following steps:

  (1.)Take a backup copy of all the needed files in NVRAM.

  (2.)Erase the entire NVRAM by **erase /all nvram:**. Now, we can make sure that there is no stale pointers existing in NVRAM by filling the NVRAM device with 0x0 or 0xFF patterns. Note: The **erase nvram:** or **write erase** commands only erase the partial contents of NVRAM.

  (3.) Now, Restore your previous files in NVRAM, to NVRAM, by "copy" and **write memory** operations.

  By this, we can ensure that this error message won't be hit in future, because of any unerased, stale pointers. Also, Kindly ensure that your image has integrated the fix for the DDTSs CSCin99301 and CSCsd13227. The DDTS CSCin98933 may trigger CSCin99301 and CSCsd13227.

- CSCin99301

  Symptoms: The router cannot be reloaded using the **reload** command. The following message is displayed when trying to reload the router:

  The startup configuration is currently being updated. Try again.

Conditions: This symptom occurs in some rare conditions. It may be triggered after the "Invalid pointer value in private configuration structure" message is displayed (as seen in (CSCin98933,CSCsd63356).

Workaround: There is no workaround other than power cycling the router.

- CSCsa63173

  Symptoms: CEF may not be updated with a new path label that is received from the BGP peer.

  If a router configured for BGP IPv4+labels multipath receives a BGP update that only changes the MPLS label for a non-bestpath multipath, the router fails to update the forwarding plane. This results in dropping or mis-branding the traffic.

  Conditions: In a IPv4+labels multipath setup, if a label is changed for the non-bestpath multipath and that is the only change in the new update received from the neighbor, the new label will not be programmed in forwarding, hence there will be label inconsistency between the BGP and the forwarding tables.

  Workaround: There is no workaround.

- CSCsb25337

  Cisco devices running Cisco IOS which support voice and are not configured for Session Initiated Protocol (SIP) are vulnerable to a crash under yet to be determined conditions, but isolated to traffic destined to User Datagram Protocol (UDP) 5060. SIP is enabled by default on all Advanced images which support voice and do not contain the fix for CSCsb25337. Devices which are properly configured for SIP processing are not vulnerable to this issue. Workarounds exist to mitigate the effects of this problem. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsb52900

  Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

  Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

  – The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
  – The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

  This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

  Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsb69271

  Symptoms: The voice path confirmation fails due to time-out while waiting for the DTMF tone.

  Conditions: The channels on the CallGen are timed-out waiting for DTMF tones, sent by the other channels. This is not specific to a particular DTMF tone, this is random.

  Workaround: There is no workaround.

- CSCsc11833

  Symptoms: An analog or digital CAS port gets into a state where inbound and/or outbound calls through the port may no longer work.

  Conditions: This symptom has been seen on Cisco 2800/3800 gateways with analog or digital CAS ports which use PVDM2 DSP modules.

It can take some time for the symptom to occur, but when it does occur, it impacts multiple ports which share the same signaling DSP. To see which DSP a port is using for signaling, check the output of the **show voice dsp signaling** exec command. It has been observed to occur more often with those ports which use DSP 1 on the PVDM2 module for signaling.

If a problem is noticed only on a single voice port, it would not be this issue.

Since PRI/BRI does not utilize the DSP for signaling purposes, it is not impacted by this issue.

When the problem occurs and this is either on a VIC2-xFXO or EVM DID/FXS modulem, run “test voice port <port #> si-reg-read 39 1” on one of the impacted ports. You need to run “terminal monitor” first to see the output. The output typically should be a single octet value for register 39. When the problem happens, information for Registers 40, 41 and 42 is presented as well and some of the registers show double-octet information. See example output below.

If using FXS or analog E&M modules, use “test voice port <port #> codec-debug 10 1” and compare the output. Again, the normal output will be single octet information for each register. See example output below.

This test only needs to be run on one of the voice ports in this state to confirm if this is the issue being seen.

Workaround: There is no workaround to prevent this problem from occurring. Once in this state, a reload of the gateway is necessary to recover it.

Additional Information: If the problem being seen has been confirmed to be this issue, the software changes associated with this report will mitigate the problem in the majority of cases. It may still be possible to see the problem in some cases and if this is experienced contact the TAC for assistance.

```
----

normal output for FXO and EVM FXS ports:
```

For FXO ports, the value is usually 0x01 but for EVM FXS this can be different. The expected output is that a single octet is displayed and only for register 39 when running the command. This command will not work on VIC-4FXS/VIC2-xFXS modules.

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#

Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x01



----
```

Output from FXO or EVM FXS port when problem occurs:

Note that the exact output for the register values will be different but when the problem happens multiple information is displayed as shown.

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
```

```
Values read from SiLabs Codec connected to DSP 0, channel 11:
-------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF


----
```

Normal output from FXS or analog E&M module. Again, please enable **terminal monitor** first to see the output. The values listed in a normal case may be different, but there should be 4 registers of a single octet only displayed.

```
Values read from PEB2465 Codec connected to DSP 02 (channel 0):
-------------------------------------------------------------
Extended Register Values (XR4..XR1) = 00, CC, 50, 11


----
```

Output from FXS or analog E&M module when problem occurs.

```
Values read from PEB2x65 Codec connected to DSP 0, channel 1:
-------------------------------------------------------------
Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCsc40236

  Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

  Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

  Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc40952

  Symptoms: Phones that are configured for Cisco VT Advantage feature will not register with SRST if they are engaged in SRST fallback operation.

  Conditions: This symptom is observed when using the following:

  - Cisco CallManager Version 5.0 (1.51.225)
  - Cisco 2600 product line for SRST
  - Cisco IOS Release 12.4

  Workaround: Unplug connection to Cisco VT Advantage.

- CSCsc58919

  Symptoms: Packets from a DMVPN tunnel with QoS pre-classification are not classified correctly on the physical interface in the child policy-map of an HQS framework. The access-lists used do not match.

  Conditions: This happens on a Cisco 1841 router running Cisco IOS Release 12.4 (4)T.

  Workaround: There are two possible workarounds:

  - Disable hardware acceleration.

  - Use static crypto-maps in place of DMVPN.

- CSCsc68262

  Symptoms: A Cisco 2821 router may crash intermittently if the router switches Encapsulating Security Payload (ESP) packets.

  Conditions: This symptom has been observed on a Cisco 2821 router when switching ESP packets.

  Workaround: There is no workaround.

- CSCsc76407

  Symptoms: Router-originated packets that are subject to encryption are bypassing the Quality of Service (QoS) feature. This prevents QoS from giving priority to protocol packets (for example BGP), which in turn can cause these protocol packets to be dropped when the outgoing link is congested.

  Conditions: This symptom is observed when router-originated packets are IPSec encrypted.

  Workaround: Disable CEF and fast switching and use process switching.

- CSCsc80670

  Symptoms: The on-board FastEthernet 0/0 results in state “FastEthernet0/0 is up, line protocol is down” after a reload, power-up or a shutdown and no shutdown operation. This is verified when the FastEthernet 0/0 is connected to media converters in series.

  This symptom is not present if the Cisco 1718 and Cisco 2950 routers are connected directly, without any media converters in between. This symptom may not be present using a media converter from other vendors.

  Conditions: This symptom has been observed connecting the on-board port of a Cisco 17xx router running Cisco IOS Release 12.3(11)T to media converters in series.

  ```
  1718(fa0/0)--media converter----------media converter--(fa 0/1)2950
  ```

  This symptom has also been observed with Cisco IOS Release 12.4(5), which is the latest available image for this platform.

  Workaround: Replace the media converter with one from another vendor.

- CSCsc81637

  Symptoms: A Cisco IOS VoIP gateway may reload unexpectedly.

  Conditions: This symptom is observed on a gateway such as a Cisco 2800 series or Cisco 3800 series that supports time-division multiplexing (TDM) hairpinning between voice modules. Under rare circumstances, the gateway may unexpectedly reload when a call is hairpinned between ports on the gateway.

  Workaround: There is no workaround.

- CSCsc90715

  Symptoms: PPPoE sessions are not established.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release version 12.4(6.3) but may also occur in other releases of Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsc94359

  Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf** *vrf-name network* command on the PE router that has mismatched labels.

- CSCsd02602

  Symptoms: All channels on a multichannel T3 port adapter may go down. The router may then reload unexpectedly due to a software forced crash. If not, all of the channels in the T3 may stay down until corrective action is taken.

  The following messages may appear one or more times in the router or VIP log:

  ```
  %CT3-3-MBOXSENDM: Failed to send msg MBOXP_MSG_T1_DISABLE
  to bay 1 firmware
  ```

  On a Cisco 7200 router, the following messages may be seen in the log:

  ```
  CT3SW WatchDog not cleared, WatchDog = 2
  CT3SW WatchDog not cleared, WatchDog = 3
  ```

  On a Cisco 7500 router, the following messages may be seen in the log:

  ```
  %CT3 5/8: Illegal Love Letter, cmd 0
  %CT3 5/9: Illegal Love Letter, cmd 0
  ```

  Conditions: This symptom affects routers using two-port multichannel T3 port adapters, the PA-MC-2T3 and the PA-MC-2T3+. The symptom occurs when one or more of the T1's in either T3 sees framing errors. One-port multichannel T3 port adapters, the PA-MC-T3 and the PA-MC-T3+, are not affected.

  Workaround: There is no workaround to prevent this problem. Possible corrective actions are listed below:

  Possible Corrective Actions for the Cisco 7200 router:

  1. Remove and reinsert the affected port adapter.
  2. Simulate removal and reinsertion with these exec mode commands in sequence: **hw-module slot** *slot- number* **stop hw-module slot** *slot- number* **start**
  3. Reload the router.

  Possible Corrective Actions for the Cisco 7500 router:

  1. Remove and reinsert the VIP with the affected port adapter.
  2. Use the configuration mode command: **microcode reload**
  3. Reload the router.

- CSCsd10975

  Symptoms: When the error message "duplicate channel names" is seen on the console, the router has to be rebooted to run Embedded Event Manager (EEM) policies again.

  Conditions: This symptom occurs when multiple EEM policies were configured and triggered on a Cisco IOS router. It could lead to the duplicate channel names error.

  Workaround: There is no workaround.

- CSCsd13227

  Symptoms: When saving the current configuration to NVRAM, the following error message is displayed:

  ```
  %Error opening nvram:/startup-config (Device or resource busy)
  ```

Conditions: This symptom is observed when the router runs Cisco IOS Release 12.4(7), Release 12.4(8)T, or later releases. Enter the **show version** command to detect the Cisco IOS release that is running on the router. This symptom occurs randomly and rarely.

This symptom may be occur when caveat CSCin98933 is present in the Cisco IOS software image.

This symptom is observed on the following platforms: Cisco 2600 series, Cisco 2800 series, Cisco 3725, Cisco 3745, Cisco 3825, Cisco 3845, Cisco RPM, Cisco RPMXF cards, and the Cisco AS5400. The symptom does not occur on the Cisco 7200 series and Cisco 7500 series routers with an RSP routers.

Workaround: Follow these steps:

1. Create a backup copy of the current configuration on a storage device other than NVRAM.
2. Reload the router.
3. Erase the “entire” NVRAM by entering the **erase /all nvram:** command.
4. Restore the configuration by copying the backup configuration to NVRAM and by entering the **copy startup-config running-config** command.

- CSCsd16977

  Symptoms: A crash can be observed by segmentation violation (SegV) on a Cisco 2651XM-V-CCME.

  Conditions: This symptom is observed occasionally when a fax is being sent through the router. This problem has been seen with Cisco IOS Releases 12.3(14) T and later versions through Cisco IOS Release 12.4(5).

  Workaround: There is no workaround.

- CSCsd19980

  Symptoms: A router that functions as a DHCP client may crash.

  Conditions: This symptom is observed on a Cisco router when you change the DHCP service through the **ip address dhcp** command or when DHCP is configured more than once.

  Possible Workaround: Before you make any changes, stop the DHCP service by entering the **no ip address dhcp** command followed by the **ip address dhcp** command.

- CSCsd24224

  Symptoms: The standby RP reloads unexpectedly because of a synchronization failure.

  Conditions: This symptom is observed when a Stateful Switchover (SSO) occurs and when the **no exception crashinfo file** *device:filename* command is in present in the configuration.

  Workaround: Enable the creation of a diagnostic file by entering the **exception crashinfo file** *device:filename* command.

- CSCsd27683

  Symptoms: A Cisco IOS H.323 gateway (GW) that is running Cisco IOS Release 12.4 (7) is not initiating the H.245 TCP connection.

  Conditions: This symptom occurs only if the terminating GW or CCM sends Alert with H.245 Address and PI=1,2,8 in response to a fastStart Setup sent from the originating GW.

  Workaround: See the following:

  – Add “progress_ind alert strip” on outgoing dial peer to TGW in OGW.
  – Configure slow start on the GWs. Under voice service VoIP, H.323 mode.

Further Problem Description: An H.323 GW initiates the FS call to another GW or CCM. In response to this, CCM or terminating GW sends slow start Alert with h245 Addr and PI=1,2,8. The phone at the originating GW expects ringing tone from the terminating GW. It is not ringing now, but the phone at the terminating side is ringing. Now if user did not pick the call (i.e. will not send Connect message), then the call will drop. Caller will never come to know what happened at the other end (there is no ringing tone). Without PI in Alert, it works well.

- CSCsd29364

  Symptoms: Service Selection Gateway (SSG) does not send attribute NAS-PORT [5] on the access request packet for a prepaid service reauthorization.

  Conditions: This symptom occurs when SSG is configured, and User is a prepaid user.

  Workaround: There is no workaround.

- CSCsd39519

  Symptoms: A Media Gateway Control Protocol (MGCP) gateway hangs when voice calls come in from either the IP or the PSTN side in which a leg of the call is on a BRI Voice Interface Card (VIC). The gateway stops responding and does not process any traffic. The only way to bring the router back is to power-cycle it.

  Conditions: This symptom is observed for every call over a BRI VIC/WIC if the MGCP gateway runs Cisco IOS Release 12.4(4)T1 or later releases. The symptom may also occur in Release 12.4.

  Workaround: There is no workaround. The symptom is not observed when the MGCP gateway runs Cisco IOS Release 12.4(4)T.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd43706

  Symptoms: A Cisco router crashes while executing the **show policy-map interface** command.

  Conditions: Configure the service policy with CBWFQ and WRED based on prec and Explicit Congestion Notification (ECN).

  Workaround: There is no workaround.

- CSCsd44118

  Symptoms: When running TCL/VXML applications that perform Media Play, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: This symptom is observed when Cisco IOS Media Play code forgets to release a memory at the end of Media Play.

  Workaround: There is no workaround. Contact Multiservices TAC (IOS) and request a patch.

- CSCsd46403

  Symptoms: Call comes into an E1 R2 line on a Cisco AS5350 or Cisco AS5400 and gets sent via H323 to an endpoint. The endpoint connects the call, but the Cisco AS5350 or Cisco AS5400 fails to TX ANSWERED on CAS leg resulting in a dead air call.

  Conditions: This symptom occurs on a Cisco AS5350 and a Cisco AS5400 that are running later releases than Cisco IOS Release 12.3(11)T9. Earlier releases are not affected. This symptom also occurs on a Cisco AS5350XM and a Cisco AS5400XM.

  Workaround: There is no a workaround.

- CSCsd51429

  Symptoms: A Cisco router that is running SNASw that has lost connectivity on an HPR-IP link shows the link state as active with the **show snasw link** command. The message "%SNASW-4-LDLC_CTRL_LOG_1: EXCEPTION - 81 - LDLC command frame retry limit exceeded" appears, but a message "%SNASW- 3-EVENT: Link station XXXX deactivated" does not. The mainframe product correctly shows the link as inactive.

  The link cannot be reactivated. Trying to stop the link with the **snasw stop link** command leaves the link in Pending Inactive state.

  Conditions: This symptom occurs when there is an outage between the SNASw router and the mainframe, such as an IP failure, interface failure, or mainframe reload.

  Workaround: There is no workaround. The SNASw subsystem must be restarted with the **snasw stop** command followed by the **snasw start** command to clear the condition.

  Further Problem Description: This problem was caused by a bad code fix in CSCej78434.

- CSCsd55779

  Symptoms: A Cisco VG224 reregisters all its ports instead of dropping the calls.

  Conditions: This problem can be seen for every call. Normal calls from an IP phone to an analogue phone that are connected to an FXS port are okay.

  Workaround: There is no workaround.

- CSCsd58220

  Symptoms: The callee's phone rings continuously even after the caller goes on- hook.

  Conditions: When the caller goes on-hook, the gateway receives idle and does not recognize the idle. The call does not get disconnected and the callee keeps hearing the ringing tone continuously.

  Workaround: The callee has to pick up the phone for the call to be dropped.

- CSCsd67958

  Symptoms: A router acting as Home Agent (HA) may crash when PIM is configured on it. The behavior is seen when a neighbor with a higher Layer3 address tries to become the Designated Router (DR).

  Conditions: The interfaces on HA and its neighbor are configured with sparse- dense mode (PIM) and Mobile IP HA created Mobile IP tunnels and deleted them. This symptom is observed on a Cisco router that is running Cisco IOS Interim Release 12.4(7.15).

  Workaround: If PIM needs to be configured on tunnel interfaces, this crash can be avoided by choosing higher values of tunnel interface number, like "interface tunnel xxxx" which might not have been created by Mobile IP for Mobile IP flows and deleted. Or, PIM needs to be configured on tunnel interfaces before Mobile IP creates any Mobile IP tunnels.

- CSCsd77528

  Symptoms: The following error message is found in Cisco 2821 routers when the v124_7_throttle image boots up:

  ```
  NV: Invalid Magic found in NVRAM.....Erase of configuration files recommended
  ```

  Conditions: This symptom is observed in Cisco 2821 routers. NVRAM should be erased using the **erase nvram:** command or the **write erase** command or the **erase /all nvram:** command or the **erase startup-config** command, with Cisco IOS Release 12.3(8)T or its earlier releases. When reloading the router with Cisco IOS Release 12.4(7) or later releases, this error message will be displayed.

  Workaround: If the **erase nvram:** command or the **write erase** command or the **erase /all nvram:** command is issued once the router boots up with Cisco IOS Release 12.4(7) or later releases, NVRAM will be brought into normal operating conditions.

Wide-Area Networking

- CSCed51827

  Symptoms: When you ping a router, the following error message is generated on the router:

  ```
  %IPFAST-2-PAKSTICK: Corrupted pak header for Virtual-Access3, flags 0x80
  ```

  Conditions: This symptom is observed when PPP Multilink (MLP) over L2TP is configured.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(7)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(7). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(7). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCea56560

  Symptoms: Configuring nonexisting NTP peers repeatedly may cause a router or switch to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router and Cisco switch that are configured for NTP.

  Workaround: Do not add and delete nonexisting NTP peers in quick succession, for example by using a cut-and-paste operation.

- CSCec75641

  Symptoms: A Cisco router may reload when there are two or more Telnet or console sessions to the router.

  Conditions: This symptom is observed when the following events occurs:

  – In one session, enter the **show ip as-path-access-list** *acl-number* command. The output pauses at the “--more--” prompt when there is more than one page output.

  - In another session, enter the **no ip as-path access-list** *acl-number* command in which the *acl-number* argument is the same one as in the **show ip as-path-access-list** *acl-number* command.
  - In the first session, type in “enter” or “space” in the first session to display the rest of the show command output.

  Workaround: Do not enter the **show ip as-path-access-list** *acl-number* command when the **no ip as-path access-list** *acl-number* command is being configured.

- 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 greater than 128 characters long. A token in a URL is the characters between two ’/’ characters. For example, in the URL http://172.16.1.1/level/7/show/, “level”, “7” and “show” are the three tokens in this URL.

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

- CSCeh25393

  Symptoms: A memory leak occurs when many VLANs are being created and deleted.

  Conditions: This symptom was observed while running a script to configure VLANs on both the switch and CSM and then delete these VLANs. At every 50 loops, results are printed from the **show memory status** command and free memory constantly decreases. After two days running and 2200 loops, free memory decreases about 4.6 megabits from the original 326 megabits

  Workaround: There is no workaround.

- CSCei34102

  Symptoms: A router that has many sessions configured crashes when interfaces flap.

  Conditions: This symptom is observed on a Cisco router that functions in a stress situation when 8000 PPPoA sessions are brought up and the interfaces flap.

  Workaround: There is no workaround.

  Further Problem Description: The router crashes when it attempts to establish 8000 PPPoA sessions and 800 tunnels for scalability characterization. When the interfaces flap for a first time, all 8000 sessions come up. The crash occurs when the interfaces flap for a second time.

- CSCei37916

  Symptoms: A Cisco GGSN does not function properly when wait-accounting and AAA Broadcast Accounting are configured on an APN. When the first RADIUS server responds to an Accounting Start message, the GGSN establishes the PDP context without waiting for responses from all other RADIUS servers. Under a stress condition, the GGSN may reload.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 and GGSN Release 5.2 and occurs only when both wait-accounting and AAA Broadcast Accounting are configured together on an APN.

  Workaround: There is no workaround.

- CSCei77083

  Symptoms: A spurious memory access may be generated on an RSP when a VIP that is in a disabled or wedged condition is recovered because of a Cbus Complex or microcode reload.

  Conditions: This symptom is observed on a Cisco 7500 series that has a VIP that is in a disabled or wedged condition after the router has booted.

  Workaround: There is no workaround.

- CSCej18051

  Symptoms: Terminal window PPP clients may fail with Cisco Access servers.

  Conditions: This symptom has been observed on Cisco AS5400 gateways and Cisco AS5800 servers.

  Workaround: There is no workaround.

- CSCej42445

  Symptoms: MS-CHAP authentication fails with Cisco IOS Release 12.4(5) and MS- CHAP and PAP authentication fails with the Cisco IOS Release 12.4(5)fc2 image

  Conditions: This symptom has been observed when running Cisco IOS Release 12.4 (5) and Release 12.4(5)fc2 while using Tacacs+ with MS chap for authentication.

  Workaround: There is no workaround.

- CSCej52211

  Symptoms: A Cisco 7100 router resets while booting.

  Conditions: This symptom has been observed only on a Cisco 7100 router with a PE port on slot1.

  Workaround: Change the PE adaptor to another port.

- CSCej59916

  Symptoms: The removal of authorization keywords for attributes that are implemented can cause some undesirable authorization failure.

  Conditions: This symptom has been observed when AAA tries to do authorization using these keywords.

  Workaround: There is no workaround.

- CSCsb08386

  Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

  Conditions: This symptom is observed on a Cisco router when BGP is being updated.

  Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb86257

  Symptoms: When a named ACL is used at a vty line on an PE router with an interface that is configured in an VPN VRF, making a Telnet connection from this VRF on the interface that is part of the VRF is accepted even though the **vrf-also** keyword is not configured in the **access-class** *access-list-number* command.

  When a regular numbered ACL is used, an incoming Telnet connection from an interface that is part of a VRF is rejected without the **vrf-also** keyword being configured in the **access-class** *access-list-number* command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an MPLS VPN environment and that has VPN VRFs configured.

  Workaround: Use a numbered ACL instead of a named ACL on vty lines on a PE router.

- CSCsc27615

  Symptoms: RSP QAERROR is seen with a VIP crash and MEMD carve due to standby OIR or another VIP crash at close intervals.

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

Workaround: There is no workaround.

Interfaces and Bridging

- CSCei39800

  Symptoms: VIP containing PA-1FE (FastEthernet) may crash when the router is reloaded or on an MTU change in any of the interfaces of a Cisco 7500 router.

  Conditions: This symptom has been observed when a Cisco 7500 with one port FastEthernet PA is reloaded and the VIP slot becomes wedged.

  Workaround: Doing a soft Online Insertion and Removal (OIR) would return the wedged VIP with 1 port FE PA to normal operation.

- CSCei68284

  Symptoms: POS interfaces may remain in the up/down state after the router has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

  Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

- CSCsa83907

  Symptoms: Layer-1 alarm handling does not meet the ANSI T1.231 standard on a PA-A3-T3 interface. The PA-A3-T3 port adapter does not provide a soaking time to declare and clear near-end failures such as LOS, LOF, and AIS. Also, PA-A3-T3 interfaces do not properly handle P-bit and C-bit errors and do not bring down the controller when the threshold is reached for such errors.

  Conditions: These symptoms are observed on a Cisco 7200 series that is configured with a PA-A3-T3 port adapter.

  Workaround: There is no workaround.

- CSCsb94350

  Symptoms: An Ethernet interface may accept packets for any destination MAC address. The router will process them and will forward them through the appropriate interface should a valid entry exists in the routing table.

  Conditions: The controller is in promiscuous mode and bridging is configured in any interface in the router. The output of **show interface** *interface irb* for the affected Ethernet interface prints the following message for all subinterfaces:

  ```
  Not bridging this sub-interface.
  ```

  Workaround: In the affected Ethernet interface: 1. Configure a subinterface with a dumb VLAN. 2. Configure bridging in that subinterface. 3. Remove the bridging configuration. 4. Remove the subinterface.

- CSCsc05213

  Symptoms: ISDN L2TP sessions cannot be brought up.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4 or Release 12.4T and that is configured with a PA-MC-8TE1+ port adapter that functions in T1 mode. The symptom is platform-independent and could also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCsc17534

  Symptoms: Unicast packets are not CEF-switched on a VIP but are fast-switched on the RP.

Conditions: This symptom is observed on a Cisco router that has a VIP only when the ingress interface is an ISL subinterface.

Workaround: There is no workaround.

- CSCsc25970

  Symptoms: While configuring the dot1q encapsulation in the router, traceback is seen.

  Conditions: This symptom has been observed with a router configured with dot1q encapsulation and IPSec.

  Workaround: There is no workaround.

- CSCsc29478

  Symptoms: Interfaces of a serial port adapter fail and do not come into service, preventing you from establishing links or tunnels via these interfaces.

  Conditions: This symptom is observed on a Cisco 7500 series that runs an interim release for Cisco IOS Release 12.0(32)S.

  Workaround: There is no workaround.

- CSCsc30369

  Symptoms: A cBus Complex Restart may occur on a Cisco 7500 series when you leave the interface configuration mode after you have changed the encapsulation on a serial interface from HDLC to another encapsulation type such as PPP or Frame Relay.

  The maximum datagram for an interface a of low-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1528 because the overhead that is added to the MTU is 28. The maximum datagram for an interface a of high-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1530 because the overhead that is added to the MTU is 30.

  When the encapsulation type is changed, the maximum datagram size may change, which causes an internal MTU change. This situation may cause some packets to be dropped as giants.

  Conditions: This symptom is observed after the first change to the type of encapsulation from the default of HDLC to another encapsulation type when you leave the interface configuration mode. Subsequent changes to the type of encapsulation do not cause the cBus Complex Restart.

  Workaround for the cBus Complex Restart: There is no workaround for the cBus Complex Restart. An MTU change on a Cisco 7500 series results in a cBus Complex Restart, which usually means a router outage of 15 to 30 seconds or a minute and a half, depending on the Cisco IOS software image that the router is running.

  Workaround for the packet drops: Reconfigure the MTU to prevent packet from being dropped as giants.

  Further Problem Description: The fix for this caveat ensures the maximum datagram for an interface a of low-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is 1608 to allow for an overhead to the MTU of 108. The maximum datagram for an interface a of high-speed serial port adapter with HDLC encapsulation and an MTU of 1500 is then 1610 to allow for an overhead to the MTU of 110.

- CSCsc57207

  Symptoms: A large number of the following error messages have been received:

  ```
  event flooding: code 1 arg0 0 arg1 0 arg2 0
  ```

  Conditions: This symptom has been observed on the Cisco 7200 router.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCec25562

  Symptoms: A Cisco router may crash while signaling 40K TE LSPs.

  Conditions: When RSVP refresh reduction is enabled and the router has exhausted its memory, then it is possible a crash may occur inside rsvp_rmsg_process_acks() if a queue element could not be allocated. The code does not check if the queue element was successfully allocated before removing a pointer to it.

  Workaround: There is no workaround.

- CSCec26626

  Symptoms: A Cisco router may crash if a message id is deleted without first being removed from the message id database.

  Conditions: This symptom has been observed when RSVP refresh reduction is enabled and the router has exhausted its memory.

  Workaround: There is no workaround.

- CSCef97738

  Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

  Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

  Workaround: Remove and add the MDT statement in the VRF.

- CSCei45669

  Symptoms: An OSPF router may update and originate a new version of an LSA when it should flush the LSA.

  Conditions: This symptom is observed on the originating router when it receives a self-originated MaxAge LSA before it can flush this LSA from its database. This symptom may occur under a rare condition when a neighboring router calculates that is has a newer copy of the LSA from the originating router and bounces the MaxAge LSA to the originating router.

  Workaround: Enter the **clear ip ospf process** command.

- CSCei77227

  Symptoms: A Cisco router that functions in a multicast VPN environment may crash.

  Conditions: This symptom is observed when you check the unicast connectivity and then unconfigure a VRF instance.

  Workaround: There is no workaround.

- CSCei93982

  Symptoms: A router that is running Cisco IOS may crash unexpectedly.

  Conditions: NAT must be enabled for this symptom to occur. The problem is seen when an application uses two well known ports: one for source and the other for destination. The outgoing translation is created, but on the return trip, using the previous source port as the destination, NAT may use the incorrect algorithm.

For example, if a PPTP session is initiated to the well known port 1723 from source port 21 (FTP), then the outgoing packet will create a FTP translation (we look at source information when going from in->out). When the packet is returned, we again look at the source information to know what kind of packet this is. In this case we have the source port will be 1723, and NAT will assume this is a PPTP packet. This will try to perform PPTP NAT operations on a data structure that NAT built for a FTP packet and may lead to a crash.

Workaround: There is no workaround.

- CSCej55183

  Symptoms: The router might crash when removing the ARPA Encapsulation from the configuration.

  Conditions: This symptom has been observed when ARPA Encapsulation is removed from the configuration.

  Workaround: There is no workaround.

- CSCej62500

  Symptoms: NAT Stateful forces the router to crash when there is heavy traffic exchanged between two peer SNAT routers. When active routers come back and a DUMP request process occurs at the same time, entries time out all together. This generates a large number of ACK packet exchanges and the actual data structure which stores these ACKs cannot handle this amount.

  Conditions: This symptom has been observed with SNAT Active/Standby configuration using the SNAT UDP option. When the NAT table has a size larger than 10000 entries, all entries of the table time out together. This timeout generates high density of packet exchange due to SNAT flow control mechanism.

  Workaround: There is no workaround.

- CSCek10384

  Symptoms: A Cisco 7200 router that is performing NAT could drop IPSec packets.

  Conditions: This symptom is observed on a Cisco 7200 router that is performing NAT functionality for IPSec transit packets. The router will NAT and forward the Inside to Outside IPSec (ESP) packets, but might drop the return IPSec packets from Outside to Inside.

  Workaround: Disable NAT for IPSec.

- CSCsb09709

  Symptoms: A router crashes because of a watchdog timeout when you remove a BGP configuration with an IPv6 Address Family Identifier (AFI).

  Conditions: This symptom is observed when you enter the **no router bgp** command for a BGP configuration with an IPv6 AFI.

  Workaround: There is no workaround.

- CSCsb09852

  Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

  Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

  To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsb50606

  Symptoms: Memory utilization in the "Dead" process grows gradually until the memory is exhausted. The output of the **show memory dead** command shows that many "TCP CBs" re allocated. Analysis shows that these are TCP descriptors for non-existing active BGP connections.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13), that has an NPE-G1, and that functions as a PE router with many BGP neighbors. The symptom may not be platform-specific.

  Workaround: Reload the router. I this is not an option, there is no workaround.

- CSCsb60206

  Symptoms: When an SSO switchover occurs, the newly active Supervisor Engine or RP generates a series of CPU Hog messages in the PIM Process, generates tracebacks, and finally crashes because the watchdog timer expires.

  Conditions: This symptom is observed on a Cisco switch that has redundant Supervisor Engines and on a Cisco router that has redundant RPs when Auto-RP is configured and when regular multicast traffic runs for a few hundred multicast routes.

  Workaround: There is no workaround.

- CSCsb64585

  Symptoms: A Rendezvous Point is down but multicast routing continues to function.

  Conditions: This symptom is observed when a statically mapped Rendezvous Point is defined as an interface address and when the interface is in the down/down state. In this situation, the router still attempts to become the Rendezvous Point for the defined group or groups.

  Workaround: Do not use a a statically mapped Rendezvous Point. Rather, configure Auto-RP or BSR to configure a dynamic Rendezvous Point.

- CSCsb86290

  When using ip nat service fullrange udp port 500, port ranges are broken. If source port is higher than 1024 the PAT port should be also higher then 1024 but is sometimes smaller.

  This causes issues with Mobile IP registrations where clients send registration requests with Source Port 1434. If it is PATed with a port smaller than 1024 then MobileIP connections are not translated back to the client.

  This seen in 12.3(8)T5 but also in latest 12.4 code.

- CSCsc07467

  Symptoms: An OSPF route is lost after an interface flaps.

  Conditions: This symptom is observed rarely when all of the following conditions are present:

  – There is a very brief (shorter than 500 ms) interface flap on a point-to-point interface such as a POS interface.

  – The flap is not noticed by the neighbor, so the neighbors interface remains up.

  – The OSPF adjacency goes down and comes back up very quickly (the total time is shorter than 500 ms).

  – OSPF runs an SPF during this period and, based on the transient adjacency information, removes routes via this adjacency.

  - The OSPF LSA generation is delayed because of LSA throttling. When the LSA throttle timer expires and the LSA is built, the LSA appears unchanged.

  Workaround: Increase the carrier-delay time for the interface to about 1 second or longer.

  Alternate Workaround: Use an LSA build time shorter than the time that it takes for an adjacency to come up completely.

- CSCsc10494

  Symptoms: When an inter-area, external, or Not-So-Stubby Area (NSSA) route is learned via a link state update that follows the initial database synchronization, the route may not be added to the routing table by a partial shortest path first (SPF) computation even though the LSA is installed in the link state database. A subsequent full SPF computation causes the route to be added.

  Conditions: This symptom is observed on a Cisco router and is most likely to occur when a large number of type 3, type 5, or type 7 LSAs are advertised and withdrawn.

  Workaround: Trigger an action that causes a full SPF computation.

- CSCsc36517

  Symptoms: A router reloads unexpectedly when a continue statement is used in an outbound route map.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: There is no workaround.

- CSCsc41694

  Symptoms: Router hangs while unconfiguring the BGP **no router bgp** command.

  Conditions: This symptom has been observed in Cisco AS5400 and Cisco AS5850 routers having the image c5400-js-mz.123-16.15

  Workaround: There is no workaround.

- CSCsc49741

  Symptoms: A router may crash when OSPFv3 is enabled.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCei47926. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCei47926. 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.

- CSCsc59089

  Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

  Conditions: This symptom is observed under the following conditions:

  - The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.
  - The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.
  - The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

  In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

- CSCsc73436

  Symptoms: High CPU usage may occur and the table versions of BGP peers are reset to zero.

  Conditions: This symptom is observed when you update a complex policy on a Cisco router that has a complex configuration of BGP peers.

  Workaround: There is no workaround.

ISO CLNS

- CSCsb07279

  Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S.

  Workaround: To have a change take effect immediately, enter the **no redistribute route-map** command followed by the **redistribute route-map** command for the IS-IS router process.

Miscellaneous

- CSCea73586

  Symptoms: The FlexWAN linecard crashes when dLFIoATM is configured under traffic.

  Conditions: This symptom has been observed with the configuration of dLFIoATM under traffic on a Cisco 7500 or Cisco 7600 platform.

  Workaround: There is no workaround.

  Further Description: Configuration of dLFIoATM when traffic is stopped should prevent the crash and then later traffic should be alright.

- CSCec11488

  Symptoms: A Network Processing Engine G1 (NPE-G1) may reload unexpectedly when a redzone overrun error occurs.

  Conditions: This symptom is observed on a Cisco 7200 series that has an ATM subinterface on which the **atm arp-server nsap** *nsap-address* interface configuration command is enabled.

  Workaround: Disable the **atm arp-server nsap** *nsap-address* interface configuration command on the ATM subinterface.

- CSCec16597

  Symptoms: Cisco CallManager controlled MGCP gateways configuration download function always configures “mgcp fax t38 inhibit”. If this is changed manually in the Cisco IOS CLI, the configuration download facility will change it back to “mgcp fax t38 inhibit”.

  This DDTS removes the code that automatically configures this line.

If customers are using CCM MGCP fax relay between gateways that are running older Cisco IOS versions, and the Cisco IOS 12.4T version with this change, the fax connections originating from the gateways that are running previous Cisco IOS versions and terminating on the Cisco IOS Release 12.4T gateway will fail unless "mgcp fax t38 inhibit" is configured on the Cisco IOS Release 12.4T gateway.

If all gateways in the customer network are running the new Cisco IOS 12.4T version with this fix, then they may configure whichever mode as desired.

With the fix to CSCec16597, the configuration utility will neither add nor remove this CLI statement.

Conditions: There are no conditions.

Workaround: Use the following command to enable and disable Cisco fax relay:

[no] ccm-manager fax protocol cisco

- CSCed92837

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the standby Route Switch Processor (RSP) my hang just before downloading the image. This situation may prevent the router from entering the STANDBY-HOT state and from being capable to perform a switchover until the standby RSP is reset.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S or 12.2 S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround. After the problem occurs, you can recover the router by either waiting for an IPC timer to expire (the default time is 30 minutes) or by entering the **hw-module sec-cpu reset** command.

- CSCee15581

  Symptoms: A router that is configured for L2VPN may crash.

  Conditions: This symptom is observed when L2VPN connections are dynamically deconfigured and then reconfigured.

  Workaround: There is no workaround.

- 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.

- CSCee69887

  Symptoms: A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the **show clns neighbors** command indicates that a certain system interface remains in the "Init" state indefinitely, although the output of the **show ip interface brief** command shows that this interface is up.

  Conditions: This symptom is observed when a dual SRP ring is configured on three routers that run Cisco IOS Release 12.2S. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg07617

  Symptoms: The following error message and spurious memory access may be generated on a Cisco 7500 series or Cisco 7600 series that is configured for dMLFR.

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x418FC0E0 reading 0x8
%ALIGN-3-TRACE: -Traceback= 418FC0E0 4026B644 40699284 40699A3C 40699368 40E80B84
40E7215C 4068A8AC
```

Conditions: This symptom is observed immediately after an MFR interface is created, after a switchover has occurred, or when a link flaps continuously.

Workaround: There is no workaround.

- CSCeh08545

  Symptoms: A router that performs a dynamic DNS update to remove a host name may crash.

  Conditions: This symptom is observed on a Cisco router when an interface that is configured to use dynamic DNS updates and acquire an IP address via DHCP has the **no ip-address** command enabled.

  Workaround: There is no workaround.

- CSCeh18306

  Symptoms: On a Cisco 2600-XM series that is configured with an AIM-ATM module, when one PVC is configured for ABR and another PVC is configured for another ATM class, CRC errors occur on the far end of the ATM link of the PVC that is configured for the other ATM class. This situation may occur because the PVC that is configured for ABR sends two RM cells in a row and overwrites some data of the PVC that is configured for the other ATM class

  Conditions: This symptom is observed on a Cisco 2651-XM that runs Cisco IOS Release 12.3 and that is configured with an AIM-ATM module. However, the symptom may not be platform-dependent and may occur on any platform that is configured with an AIM-ATM module.

  Workaround: Do not configure ABR on a PVC.

- CSCeh42472

  Symptoms: On a Cisco 7500 series that has redundant RSPs and that is configured for RPR, RPR+, or SSO, the standby RSP may fail to boot and may generate the following error message:

  Error : Uncompression of the image failed. Compressed image needs larger DRAM space

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2S or Release 12.4 when any of the following conditions occur:

  – The standby RSP has 128 MB of memory and the difference between the uncompressed Cisco IOS software image size and compressed Cisco IOS software image size is larger than 32 MB.
  – The standby RSP has 256 MB, 512 MB, or 1 GB of memory and the difference between the uncompressed Cisco IOS software image size and Cisco IOS compressed software image size is larger than 68 MB.
  – The standby RSP has memory of another size than what is mentioned above and the difference between the uncompressed Cisco IOS software image size and compressed Cisco IOS software image size is larger than 24 MB.
  – The standby RSP memory is smaller than 128 MB.

  Workaround: Upgrade the memory of the standby RSP so that the above-mentioned memory constraints are not applicable.

- CSCeh88604

  Symptoms: One or more VIP slot controllers reset.

Conditions: This symptom is observed on a Cisco 7500 series when the **ip nbar protocol-discovery** command is enabled. The symptom may not be platform-dependent and may also occur on other platforms in a similar configuration.

Workaround: Disable protocol discovery by entering the **no ip nbar protocol-discovery** command.

- CSCei30764

  Symptoms: A PE router that is configured with many (100 or more) Multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF.

  Conditions: This symptom is observed when you reload a Cisco router that functions as a PE router and that is configured for MVPN.

  Workaround: There is no workaround.

- CSCei40573

  Symptoms: A router that is configured as a Secure Device Provisioning (SDP) server may crash.

  Conditions: This symptom is observed when the router uses a configuration template that is larger than 14,386 bytes.

  Workaround: Do not use a configuration template larger than 14,386 bytes. Rather, reduce the size of the configuration template so that it includes only the modifications that must be made to the existing configuration.

- CSCei40803

  Symptoms: When tunnel protection is enabled, an inbound ACL is processed twice, once before the decryption and once after the decryption, which you can see in the output of the **show access-lists** [*access-list-number*]|[*access-list-name*] command.

  Conditions: This symptom is observed on a Cisco router that has tunnel protection enabled for IPSec + GRE tunnels.

  Workaround: Add an ACL entry to permit the incoming GRE packets or use a crypto-map instead of tunnel protection.

- CSCei48251

  Symptoms: A router that is configured for Pseudowire Redundancy may and generate the following stack trace:

  ```
  FP: 0x4581CE80[etext(0x42316c92)+0x35061ee], RA: 0x4154B924
  [atom_seg_packet_process_send_func(0x4154b81c)+0x108] FP:
  0x4581CEC0[etext(0x42316c92)+0x350622e], RA: 0x4045A87C[sss_switch_pak
  (0x4045a5d8)+0x2a4] FP: 0x4581CF50[etext(0x42316c92)+0x35062be], RA: 0x418CDA98
  [ac_vlan_switching_receive_pak_process(0x418cd924)+0x174] FP:
  0x4581CFA0[etext(0x42316c92)+0x350630e], RA: 0x418CC1DC
  [ac_switching_receive_pak_process(0x418cbfec)+0x1f0] FP:
  0x4581D008[etext(0x42316c92)+0x3506376], RA: 0x418CC920[acswitch_process
  (0x418cc8a4)+0x7c]
  ```

  Conditions: This symptom is observed on a Cisco router that has one AToM and one non-AToM segment.

  Workaround: There is no workaround.

- CSCei51142

  Symptoms: A CA server that is rebooted may reset the issued serial number to 1, thus re-issuing a certificate with the same serial number.

  Conditions: This symptom is observed on Cisco routers such as a Cisco 1841 and Cisco 2811 that have a built-in hardware clock.

Workaround: There is no workaround.

- CSCei62522

  Symptoms: ISAKMP SA negotiation is not successful in aggressive mode.

  Condition: This symptom has been observed when testing Radius Tunnel Attribute with HUB and Spoke Scenario using Cisco IOS interim Release 12.4(3.3).

  Workaround: There is no workaround.

- CSCei62952

  Symptoms: A Cisco device running IOS may drop traffic because the routing table and the CEF forwarding table are inconsistent. This problem is exposed when the routing table is reloaded by clearing the routing table or on a box that supports hardware forwarding resetting the forwarding complex. ie: PXF. This is a rare situation due to the prefix distribution and timing required to expose the condition.

  Workaround: None.

- CSCei75828

  Symptoms: The following error message is seen on a router configured with a large number of IPv6 VLANs (i.e., several thousand) and a similarly large number of IPv6 recursive static routes when the state of the physical interface changes:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (nn/nn),process
  = Exec.
  ```

  Conditions: System is configured with a large number of IPv6 VLANs. System is also configured with a large number of IPv6 recursive static routes, resolving through the VLAN prefixes. State change occurs on physical interface associated with VLANs.

  Workaround: Replacing IPv6 recursive static routes with IPv6 fully-specified static routes may alleviate this problem.

- CSCei76610

  Symptoms: A router running a VXML application crashes.

  Conditions: This symptom has been observed with a router receives an oversize cookie from the HTTP server.

  Workaround: Reduce the HTTP cookie size to under 240 bytes.

- CSCei82163

  Symptoms: A Cisco AS5400 might not release all voice resources for an MGCP call after it is disconnected.

  Conditions: This symptom is observed on both the Cisco AS5400 and Cisco AS5850 platforms but is not platform dependent. The symptom is associated with the simultaneous disconnection of a large number of calls.

  Workaround: There is no workaround.

- CSCej00319

  Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured or removed from an interface or globally.

  Conditions: This symptom is observed when parallel links are present.

  Workaround: There is no workaround.

- CSCej13460

  Symptoms: The packets are not switched correctly using the Fast Switching with IPSec tunnel protection feature.

  Condition: This symptom has been observed in Cisco IOS Release 12.4(1b) when tunnel protection IPSec is configured and tunnel source interface has Fast- switching (but not CEF) configured.

  Workaround: Use CEF switching.

- CSCej20505

  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

- CSCej22786

  Symptoms: A Cisco AS5850 universal gateway reloads unexpectedly with a traceback while voice calls and fax calls are brought up simultaneously.

  Conditions: This symptom has been observed when bringing up more than 500 SIP and H.323 voice calls and 92 T.38 Fax Relay calls.

  Workaround: Bring up voice calls only; do not bring up fax calls.

- CSCej27710

  Symptoms: The voicemail box is not available.

  Conditions: This symptom has been observed when a mailbox is assigned to a phone and someone leaves voice mail.

  Workaround: There is no workaround.

- CSCej35355

  Symptoms: A voice port remains in the S_OPEN_PEND state, preventing a trunk from coming up.

  Conditions: This symptom is observed on a Cisco 2600 series when the voice port is configured via a T1 controller. The symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCej42480

  Symptoms: Incoming or outgoing PSTN calls fail on a PRI interface.

Conditions: This symptom has been observed on a Cisco 2620XM VoIP Gateway (MGCP) with Cisco IOS Release 12.4(2)T1 and a PRI Backhauled MGCP Gateway controlled by Cisco CallManager Release 4.1(3)SR1.

Workaround: There is no workaround.

- CSCej42804

  Symptoms: A Cisco Gateway that is running Session Initiation Protocol (SIP) calls might run out of processor memory due to hung SIP calls.

  Conditions: Active and hung calls can be seen using the **show sip-ua calls** command. The following specific scenario will result in a hung call: 1) The gateway initiates an INVITE. 2) The gateway receives a 100/180 response. 3) The gateway sends a CANCEL. 4) The gateway receives the 200ok for the CANCEL. 5) The gateway receives an invalid final response for the INVITE (or no final response) and drops the message.

  Each hung call will use a little more memory, and eventually the gateway will run out of memory.

  Workaround: Downgrade to Cisco IOS Release 12.3(14)T3, Release 12.3(11)T6, Release 12.4(2)T1, or Release 12.4(1a).

- CSCej42935

  Symptoms: Data corruption may occur on a disk when directory entries are read by more than one process simultaneously.

  Conditions: This symptom is observed on a Cisco platform that has an ATA file system when, for example, the **dir disk0:** command is entered on one vty connection and simultaneously, and for the same disk, the **copy disk0:** command is entered on another vty connection.

  Workaround: There is no workaround.

- CSCej43220

  Symptoms: A Cisco 7200 router terminating Remote IPSec Clients using IPSec Dynamic Virtual Interface could cause a delay of 10 seconds in bringing up the tunnel.

  Conditions: This symptom has been observed with a Cisco 7200 router using IPSec Dynamic Virtual Interfaces to terminate Remote VPN Clients. When the client tries to establish the IPSec tunnel, the Cisco 7200 hub responds to Phase1 IKE immediately, but could delay Phase2 IPSec Quick Mode by 10 seconds. The Cisco 7200 could wait for 10 seconds before responding to the QM negotiation.

  Workaround: There is no workaround.

- CSCej43787

  Symptoms: Issuing a **no mgcp** command reloads the network access server (NAS) unexpectedly. The MGCP gateway crashes and reloads due to Hairpin calls.

  Conditions: The unexpected reload is seen while issuing **no mgcp** command after stress testing. This symptom has been observed on a Cisco AS5850 platform running Cisco IOS Release 12.4(5) and only in an MGCP environment when Hairpin calls are involved.

  Workaround: There is no workaround.

- CSCej50928

  Symptoms: Media Gateway Control Protocol (MGCP) calls fail to land in timeslots 16-31 on E1 controllers.

  Conditions: This symptom is observed in a Cisco AS5850 platform that is running a Cisco IOS Release 12.4(5) image. This symptom is not observed if OGW is a Cisco AS5400 platform. This was not observed in a Cisco IOS Release 12.4 (3.8) image. This may be service impacting as only half of the timeslots can be used for generating calls.

Workaround: There is no workaround.

- CSCej53240

  Symptoms: The system can run out of memory with voice calls over a period of time. With the system handling a large number of voice calls (greater than 50), running the **show memory summary** command periodically will indicate memory in use is increasing.

  Under these conditions, the **show memory debug leak chunks** command shows that there is a memory leak.

  A sample output of this command when the problem is seen is shown below:

```
Chunk Elements:
Address  Size  Parent   Name
45ACC8C8  2052 45786824 (VTSP EVENT poo)
45ACD0D0  2052 45786824 (VTSP EVENT poo)
45ACD8D8  2052 45786824 (VTSP EVENT poo)
```

  Conditions: This issue is likely to be seen when the system is handling a large number of voice calls (greater than 50). This issue is present in Cisco IOS Release 12.4(5).

  Workaround: Reload the system to recover from this condition.

- CSCej59173

  Symptoms: Class-map queueing information is incorrectly shown under the policy- map on the output interface.

  Conditions: This symptom has been observed under the following conditions:

  1. Configure the **class-map** command and attach bandwidth to it.
  2. Configure the **service-policy** command.
  3. Enter the **show output policy-map** command.

  Workaround: There is no workaround.

- CSCej83415

  Symptoms: A Cisco IOS gateway might crash while running voice calls.

  Conditions: This symptom is observed under high stress/high CPU where race conditions in Cisco IOS are more likely to occur. These race conditions can result in a MIBS data base corruption or RTP memory corruption resulting in a crash.

  Workaround: There is no workaround.

- CSCej83614

  Symptoms: Multicast packets are punted to the RP instead of being fast-dropped.

  Conditions: This symptom is observed on a Cisco router when an access control list is configured on the egress interface to deny all IP packets.

  Workaround: There is no workaround.

- CSCek01162

  Symptoms: When removing the OSPF IPsec authentication configuration from CLI in IPV6, an alignment traceback will be seen pointing back to crypto_ikmp_peer_is_dead.

  Conditions: This symptom occurs when OSPF IPsec authentication (IPV6) is configured and removed.

  Workaround: There is no workaround.

- CSCek13657

  Symptoms: The following error message may be generated when a router boots:

  ```
  %SYS-2-NULLCHUNK: Memory requested from Null Chunk
  -Process= "Init", ipl= 3, pid= 3  with an accompanying traceback.
  ```

  Conditions: This symptom is platform- and release-independent and occurs when the router boots.

  Workaround: There is no workaround. However, proper system operation is not affected.

- CSCin80221

  Symptoms: A Cisco router crashes when you enter the **fsck** command for an ATA flash disk.

  Conditions: This symptom is observed when the boot sector of the ATA flash disk is corrupted and when the router runs a release that is listed in the "First Fixed-in Version" field at http://www.cisco.com/cgi- bin/Support/Bugtool/onebug.pl?bugid=CSCed58384. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Format the disk.

- CSCin88771

  Symptoms: A router hangs while writing a crashinfo to a disk.

  Conditions: This symptom is observed on a Cisco router that is configured with an ATA file system when the memory is corrupted. The router is unable to save MALLOC requests to a disk because the memory on the disk is corrupted, causing the router to hang.

  Workaround: Configure the router in such a way that the crashinfo is written to bootflash memory. Ensure that there is sufficient space in the bootflash memory for the crashinfo.

- CSCin97574

  Symptoms: Service Selection Gateway (SSG) sends invalid Radius Access Reject packet to a network access server (NAS).

  Conditions: This symptom is seen with SSG in radius proxy mode when AAA server is unreachable.

  Workaround: There is no workaround.

- CSCin97815

  Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

  The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in the **show frame-relay pvc** command show the packets correctly.

  Conditions: A map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

  Workaround: There is no workaround.

- CSCsa53334

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml.

- CSCsa75285

  Symptoms: A Cisco switch or router may crash when you install a 1-port multichannel STM-1, single mode port adapter (PA-MC-STM-1SMI) in a FlexWAN or VIP.

  Conditions: This symptom is observed when you first power down the switch or router, install the PA-MC-STM-1SMI, and then boot up the switch or router.

  Workaround: Install the PA-MC-STM-1SMI via an OIR procedure.

- CSCsb00759

  Symptoms: A Cisco 3640 or Cisco 3660 stops encrypting GRE packets, which are then sent in the clear.

  Conditions: This symptom is observed on a Cisco 3640 and Cisco 3660 that run Cisco IOS Release 12.3(13), that are configured for CEF, and that have an interface (but not necessarily the interface with the crypto map) that has the **ip tcp header-compression** command enabled.

  Workaround: Re-apply the service policy on the interface that is configured with the crypto map.

  First Alternate Workaround: Enter the **no route-cache cef** command followed by the **route-cache cef** command.

  Second Alternate Workaround: Delete the crypto map from the interface and re-apply the crypto map.

- CSCsb10168

  Symptoms: The Chunk Manager process holds memory, and the output of the **show processes memory** command shows the following:

  Processor Pool Total: 139794304 Used: 128152892 Free: 11641412 I/O Pool Total: 37748224 Used: 13626112 Free: 24122112

  ```
  PID TTY Allocated Freed Holding Getbufs Retbufs Process
  0 0 62756648 20964800 37337972 769 730261 *Init*
  0 0 12320 689068 12320 0 0 *Sched*
  0 0 7335084 8060988 951176 41 41 *Dead* 1 0 90389644 22896 90373720 0 0 Chunk Manager
  ```

  Conditions: This symptom is observed on a Cisco router when both the NBAR Protocol Discovery feature and NAT are configured.

  Workaround: Disable the NBAR Protocol Discovery feature.

  Additional Information: This bug requires both NAT and Crypto configuration. If the router does not have either NAT or IPsec configuration then it is safe from this bug.

- CSCsb26172

  Symptoms: When you configure “Timed Rollback,” a router reloads unexpectedly because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series.

  Workaround: There is no workaround. “Timed Rollback” is not yet supported.

- CSCsb39996

  Symptoms: The Burst size parameter in RSVP reservation for Video Calls across an IP-IP Gateway may be different from that of Video calls across an MCM Proxy. This may cause video quality problem in the associated call.

  Conditions: This symptom has been observed with Cisco IOS Release 12.3(11)T and all software releases based on Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsb42374

  Symptoms: There are two symptoms: 1. When a policy is attached to the incoming interface, an aggregate control- plane policing policy will not classify traffic correctly. 2. When a control-plane policing policy is attached to the aggregate path, a similar policy attached to the host, transit or cef-exception paths will not classify traffic correctly.

  Conditions: This symptom has been observed on a Cisco platform that runs Cisco IOS Release 12.3T or Release 12.4.

  Workaround: Any existing interface policy would have to be removed for the aggregate control-plane policing policy to work. Any existing aggregate policing policy will have to removed for the host/cef-exception/transit path control-plane policing policy to work.

- CSCsb44220

  Symptoms: During a high CPU load, the IPC ports on the RP are not opened, preventing CEF from communicating with a line card and causing a FIBDISABLE error message to be generated.

  Conditions: This symptom is observed only when the router functions under high stress (that is, there is a high CPU Load on the RP and line cards) during bootup or when you perform an OIR of a line card, RP, or SP.

  Workaround: There is no workaround.

  Further Problem Description: Caveat CSCsb83521 resolves an issue that may occur if CSCsb44220 is integrated in an image. The issue concerns a scheduler error message.

- CSCsb54961

  Symptoms: A Cisco gateway may fail to initiate a T.38 call to a third party gateway. When the third party gateway sends T.38 open logical channel to the Cisco gateway, no open logical channel acknowledgement is sent by the Cisco gateway. After waiting for 30 seconds for T.38 open logical channel acknowledgement, the third party gateway closes its T.38 open logical channel.

  Conditions: This happens when T.38 fax relay calls are originated or terminated on a Cisco gateway that is running Cisco IOS Release 12.3(4)T and later releases.

  Workaround: There is no workaround.

- CSCsb58313

  Symptoms: After running a few days, assertion failed at WA_NP_QWRITE and then crashed.

  Conditions: This symptom occurs when running the **show diag** command at high CPU.

  Workaround: Do not run the **show diag** command.

- CSCsb65867

  Symptoms: Intermittent one-way voice occurs between an IP phone and an NM-HDV2 network module.

  Conditions: This symptom is observed on a Cisco platform that functions as an MGCP gateway and that is configured with an NM-HDV2 network module.

Workaround: There is no workaround.

- CSCsb67539

  Symptoms: A Voice Gateway crashes when running under a heavy voice call load.

  Conditions: This symptom is observed on a Voice Gateway that is running Cisco IOS Release 12.3(11)T6. The gateway is under heavy voice call load with access to media/application documents residing on local gateway flash, http and tftp servers.

  Workaround: The following is not quite a workaround:

  call threshold global *cpu-5sec* **low** *value* **high** *value*

  For example:

  call threshold global *cpu-5sec* **low** *50* **high** *70*

  The CLI can ease the CPU load on the gateway by reducing the probability for a crash.

- CSCsb72138

  Symptoms: A Foreign Exchange Station (FXS) port may lock up after having functioned fine for a long time.

  Conditions: This symptom is observed on a Cisco 2821 that runs Cisco IOS Release 12.3(11)T5. This symptom typically occurs when fax lines are configured on the FXS port.

  Workaround: There is no workaround.

- CSCsb75197

  Symptoms: An SNA Switch (SNASw) rejects EE link activation with sense code 08120000. Once the SNASw runs out of ANR Labels, inbound connections, i.e. pu2.1 clients, will also be rejected with sense code 08120000 as seen on a DLCTRACE.

  Conditions: This symptom is seen when a downstream device has repeatedly sent in an old-SNA flavor of XID3 (one that indicates no exchange state indicators are supported) over an SNASw port that has not specified CONNTYPE.

  Workaround: A reload of the router will be needed to clear this condition. However, the problem can be avoided in the first place by configuring CONNTYPE NOHPR on the downstream port.

  Further Problem Description: VTAM logs show sense code 08010000 during the link activation XID3 negotiation. The SNASw shows sense code 08120000 on a DLCTRACE capture during the link activation XID3 negotiation for either upstream link activation or for an inbound device XID3 negotiation exchange during a connection attempt.

- CSCsb77885

  Symptoms: IKE negotiation will fail. Any tunnel that requires IKE to successfully negotiate a security association will not work.

  Conditions: This symptom occurs when authentication for IKE is configured as RSA encryption (authentication rsa-encr).

  Workaround: There is no workaround.

- CSCsb83521

  Symptoms: The following error message may be generated after an SSO switchover:

  ```
  %SCHED-3-STUCKMTMR: Sleep with expired managed timer 55BE2914 time 0x1CD561 (00:00:00
  ago).
  -Process= "IPC LC Port Opener" ipl= 6 pid= 166
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for High Availability (HA).

Workaround: There is no workaround.

- CSCsb83876

  Symptoms: The counters on a PA-MC-E3 port adapter may provide incorrect information. For some interfaces of the port adapter, the counters are always zero, and for others interfaces, the counters do increase but very slowly.

  Conditions: This symptom is observed when you enter the **show interfaces** *type slot* command for a PA-MC-E3 port adapter.

  Note that the symptom does not occur when you enter the **show interface** *type number* **stats** command or the **show interfaces** *type slot* **accounting** command. Also, when you enter the **show interfaces** *type slot* command for the VIP in which the PA-MC-E3 port adapter is installed, the counters provide correct information.

  Workaround: Enter the **show interface** *type number* **stats** command to retrieve the correct information.

- CSCsb85136

  Symptoms: When running TCL/VxML applications that perform Media Playing, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: Cisco IOS Media Play code was forgetting to release a memory at the end of media play.

  Workaround: Upgrade to Cisco IOS Release IOS 12.4(3b) if available. If not, contact Multiservices TAC (IOS) and request a patch.

- CSCsb86611

  Symptoms: The PPP link fails when using LQM and hardware compression.

  Conditions: This symptom has been observed on Cisco 3745 routers with AIM- COMPR4 on Cisco IOS Release 12.3(14)T2 and Release 12.4(3).

  Workaround: Use software compression, disable CEF on the ingress interface, or disable WFQ on the WAN interface.

- CSCsb87077

  Symptoms: Traffic drop is seen on WIC-1SHDSL-V3.

  Conditions: The issue happens when the WIC-1SHDSL-V3 is in line-mode auto mode. We have not seen this dropping conditions in 2-wire line-mode.

  Workaround: There is no workaround for this issue if you want to use 4-wire mode.

- CSCsb90264

  Symptoms: Cisco AS5400 and AS5350 T1 CAS calls fail with “no users answer,” and a traceback is seen at vtsp_tsp_call_setup_ind, along with the following error:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
  ```

  Conditions: This problem is seen when making CAS calls in Cisco AS5400 and AS5350 platforms.

  Workaround: There is no workaround.

- CSCsb91678

  Symptoms: A software-forced crash may occur on a Cisco 7206VXR because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco 7206VXR that has a low-speed Mueslix-based serial port adapter such as a PA-4T+, PA-8T-V35, PA-8T-X21, or PA-8T-232 port adapter and that runs a Cisco IOS image that integrates the fix for caveat CSCec63468.

The symptom occurs only for low-speed port adapters such as the PA-4T+, PA-8T-V35, PA-8T-X21, and PA-8T-232 port adapters. The symptom may also affect port adapters in adjacent slots, and not only the port adapters in physically adjacent slots, but also the port adapters that are logically adjacent in the initialization path. This memory corruption occurs in the PCI/IO memory space.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec63468. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: There is no workaround. Note that high-speed or unchannelized serial port adapters are not affected.

Further Problem Description: The following error messages and tracebacks are generated just before the crash occurs:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0 -Traceback= 6074F79C
601BB3AC 601BC72C

%MUESLIX-1-HALT: Mx serial: Serial2/0 TPU halted: cause 0x3 status 0x0043404F shadow
0x630FB864

%ALIGN-3-SPURIOUS: Spurious memory access made at 0x6074F388 reading 0x1F
%ALIGN-3-TRACE: -Traceback= 6074F388 601BB3AC 601BC72C 00000000 00000000 00000000
00000000 00000000 %ALIGN-3-TRACE: -Traceback= 6074F7C0 601BB3AC 601BC72C 00000000
00000000 00000000 00000000 00000000

%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
-Traceback= 607E0078 607E44AC 607DACD0 601B0CD4 601B1A04 601ADEA8 603E2C2C 607CF128
6076E2EC
```

- CSCsb91807

  Symptom: The memory utilization increases.

  Conditions: This symptom has been observed when SSG along with a service profile attribute of "attribute 26 9 251 "Z"" is configured.

  Workaround: There is no workaround.

- CSCsb92920

  Symptoms: A router that is configured for IPHC may crash when you remove a service policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4 or 12.4T but may also occur on other platforms. The symptom occurs when you enter the following sequence of commands:

```
frame-relay switching

class-map match-all voip
 match protocol ip

policy-map p1
 class voip
  compress header ip

interface Serial6/0
 encapsulation frame-relay
 service-policy output p1
no shutdown

interface Serial6/0
```

```
shutdown
no  service-policy output p1
no  encapsulation frame-relay
```

Workaround: There is no workaround.

- CSCsb93316

  Symptoms: In dual RP systems or in RP/SP systems, the system may crash with a Segmentation violation error.

  Conditions: This symptom has been observed only in dual RP or RP/SP systems with High availability features present. The crash may be observed when the **show file system** command is issued.

  Workaround: There is no workaround.

- CSCsb96968

  Symptoms: SSG TCP redirection does not occur.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG and occurs for prepaid users.

  Workaround: There is no workaround.

- CSCsb97185

  Symptoms: A router configured with a 36-port EtherSwitch Module may reload due to memory corruption in the I/O memory pool.

  Conditions: The router must have a 36-port ESW module.

  Workaround: Disable the **ip igmp snooping** command.

```
Router(config)#no ip igmp snooping
Router#show ip igmp snooping vlan 1
IGMP snooping is globally disabled
IGMP snooping is disabled on this Vlan
IGMP snooping immediate-leave is disabled on this Vlan
IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

- CSCsb98254

  Symptoms: A router may fail when you reload a Gigabit Ethernet (GE) line card or port adapter that has link-bundling enabled.

  Conditions: This symptom is observed on a Cisco router when dot1q is configured on a GE interface of the line card or port adapter and when MPLS is enabled on an uplink.

  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.

- CSCsb99256

  Symptoms: A Cisco 7500 series may pause indefinitely during the boot process right after the image is successfully decompressed.

  Conditions: This symptom is observed on a Cisco 7500 series that is booted with Cisco IOS interim Release 12.4(4.8). The symptom could also occur in Release 12.4T.

  Workaround: There is no workaround.

- CSCsb99906

  Symptoms: A host name domain lookup takes too long, the following error message is generated, and the CP-to-CP session is terminated:

  ```
  %SNASW-4-CPUUsage: SNASw process, type 0x603 ran for 18000 ms processing IPS of type
  0x5103, address 0x65D1DC30
  ```

  Conditions: This symptom is observed on a Cisco platform that functions as a SNASwitch and that runs Cisco IOS Release 12.4(1a).

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3.

- CSCsc00587

  Symptoms: PRI backhauled to MGCP cannot fallback into h323 mode for SRST as there is a hung call. It can be seen in the **show call active voice brief** command but if there is no calls there, definitely check the **show voice vtsp call** command. There will be a call in "S_WAIT_RELEASE" state and cannot be cleared even though ISDN status shows no active calls on that PRI.

  Conditions: This symptom is normally seen when connection from a gateway to CCM flaps. If a call hits the gateway during a transition (fallback switchover or vice versa), the call gets stuck and causes all other PRIs to clock up. The PRI is able to be backhauled to CCM with a hung call but it is not able to fallback into SRST (gateway terminated). With just one call hung, all other backhauled PRIs are affected and cannot fallback in h323. Calls inbound get a "fast busy--- isdn setup" message and is ignored by the gateway as it thinks PRI is still backhauled, so the PRIs are in limbo.

  Workaround: Reload the router.

- 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.

- CSCsc02623

  Symptom: The console locks under an aggressive syn flood attack. The **scheduler allocate 20000 1000** command is not set in a Cisco 2801 configuration by default.

  Conditions: This symptom has been observed on a Cisco 2801 router.

  Workaround: Manually enter the **scheduler allocate 20000 1000 command in the Cisco 2801 configuration after the initial configuration.**

- CSCsc02825

  Symptoms: In Cisco IOS software that is running the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the router could reload while trying to access a bad virtual address.

  Conditions: This symptom may be observed when LDP is being used. It will not be observed with TDP. It may happen when LDP receives a protocol message larger than 512 bytes right after receiving several Label Mapping messages smaller than 25 bytes. This problem is likely to be accompanied by the presence of one of the following error message:

  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xD0D0D0D

  The above error message may be preceded by one of the following four error messages:

  ```
  %ALIGN-1-FATAL: Corrupted program counter 19:45:07 CET Mon Sep 26 2005 pc=0xD0D0D0D,
  ra=0x61164128, sp=0x64879B98
  ```

  ```
  %TDP-3-BAD_PIE: peer x.x.x.x; unknown pie type 0x11E
  ```

  ```
  %TDP-3-UNEXPECTED_PIE: peer x.x.x.x unexpected pie type 0x0
  ```

  ```
  %TDP-3-PTCLREAD: peer x.xx.x0, read failure
  ```

  This problem may be seen in releases that include the fix for CSCeg74562 but do not have the fix associated with this defect.

  Workaround: There is no workaround.

- CSCsc03569

  Symptoms: Incoming and outgoing PSTN calls fail on a BRI interface.

  Conditions: This symptom has been observed on a Cisco 2620XM VoIP Gateway (MGCP) with Cisco IOS Release 12.4(2)T1 and a BRI Backhauled MGCP Gateway controlled by Cisco CallManager release 4.1(3)SR1.

  Workaround: There is no workaround.

- CSCsc09246

  Symptoms: The following commands used for detecting memory leaks would crash the router which uses external memory such as the RPM-XF platforms.

  show memory debug leaks

  show memory debug leaks chunks

  show memory debug leaks largest

  show memory debug leaks summary

  Conditions: This symptom has been observed on the RPM-XF cards using Cisco IOS interim Release 12.4(4.6).

  Workaround: There is no workaround.

- CSCsc12098

  Symptoms: The fix for busyout *slot* on the Cisco AS5400 platform causes build issues.

  Conditions: This symptom is observed on a Cisco AS5400 platform.

Workaround: There is no workaround.

- CSCsc12490

  Symptoms: When the ISDN link backup of the router comes up, the router loses memory extremely quickly, and crashes.

  Conditions: Main link goes down, which brings up the ISDN properly. Once OSPF is established, memory starts leaking at an alarming rate through “Skinny MOH Server”.

  Workaround: Keep the main link stable.

- CSCsc12570

  Symptoms: The codec upspeed (i.e., G729 to G711ulaw) or downspeed (i.e., G711ulaw to G729) does not happen. Other packet stream-related call parameter changes, such as VAD and PLAYOUT, do not happen as expected.

  Conditions: This symptom has been observed when the codec type or other packet stream parameters are modified using MDCX or through the TDM side of the call module like VTSP.

  Workaround: There is no workaround.

- CSCsc12575

  Symptom: An EzVPN tunnel fails to come up if there is certificate authentication configured.

  Conditions: Configuring the certificate authentication causes the problem.

  Workaround: Use pre-shared key authentication.

- CSCsc13844

  Symptoms: After loading "flash:c2600-entservicesk9-mz.123-11.T7.bin", the E1 controller is missing from the **snmpwalk** command of IF-MIB.

  Conditions: This symptom has been observed on a Cisco2621XM.

  Workaround: There is no workaround.

- CSCsc13998

  Symptoms: When receiving an incoming call, if an FXS port goes offhook and quickly (within 500ms) goes back onhook, the port stays in the busy state - not able to accept incoming/outgoing calls though the phone is onhook.

  Conditions: This behavior is observed on all analog FXS ports on Cisco 1700, Cisco 1800, Cisco 2400, Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 platforms. This defect will not occur in any FXO port.

  Workaround:

  1. The port can be taken out of the busy state and back to normal idle and operational state by doing an offhook follow by an onhook.
  2. Enter the **shutdown** and **no shutdown** commands and the FXS port will return to normal.

- CSCsc14106

  Symptoms: If the called party answers a call in the middle of a prompt, one- way voice occurs.

  Conditions: This symptom has been observed when a TCL application tried to play a prompt while a call is alerting and the call is answered before the prompt play is complete. If the call is answered after the prompt play is done, the symptom is not seen.

  Workaround: In the script, connection destroy and reconnect are handled to make sure a reconnect happens. This symptom is now fixed in Cisco IOS.

- CSCsc15366

  Symptoms: If a Media Gateway Control Protocol (MGCP) Create Connection (CRCX) request is received containing a request for a clear-channel codec, the Cisco 1760 router fails to find a matching codec, and the call fails.

  Conditions: This symptom has been observed on a Cisco 1760 router.

  Workaround: There is no workaround.

- CSCsc19265

  Symptoms: Standby reboots and gets stuck after 4 to 8 reloads.

  Conditions: dLFIoLL is configured with RPR+ and the MTU size is changed.

  Workaround: Change the MTU back to the default value.

- CSCsc19728

  Symptoms: The router crashes while unconfiguring **resource-pool profile customer** *word* command.

  Conditions: This symptom has been observed on Cisco AS5400 gateway containing the c5400-js-mz.124-5.2.T image.

  Workaround: There is no workaround.

- CSCsc20062

  Symptoms: A Cisco IOS router configured with Cisco IOS IPS may reload after a new signature file (SDF) is loaded on the router.

  Conditions: There are two ways to load a new signature file on the router. Conditions leading to the reload are different based on which method is used:

  1. When using this method, no other conditions need to be met.

  Execute the **copy** *url* **ips- sdf** command.

  2. When using this method, the conditions necessary for a reload are when any global **inspect** parameters are configured in the Cisco IOS configuration.

  a. Remove all configured **ip ips sdf location** commands.

  b. Configure the **ip ips sdf location** *url* command.

  c. Place the new signature file at the *url* argument.

  d. Unconfigure ips from all interfaces.

  e. Reconfigure ips on the appropriate interfaces.

  Workaround: Use method 2 above to load the signature file with the following modifications.

  a. Remove all configured **ip ips sdf location** commands.

  b. Configure the **ip ips sdf location** *url* command.

  c. Place the new signature file at the *url* argument.

  d. Unconfigure ips from all interfaces

  e. Unconfigure all global **inspect** parameters

  f. Reconfigure ips on the appropriate interfaces

  g. Reconfigure the global **inspect** parameters

- CSCsc20149

  Symptoms: When you enter the **show voice call status** command five to six times in quick succession, the CPU use of a Cisco AS5850 reaches 99 percent. The Cisco AS5850 thereafter becomes very unstable in accepting incoming calls. This situation can be highly service-impacting under stress conditions.

  Conditions: This symptom is observed on a Cisco AS5850 that is running a special image of Cisco IOS Release 12.3(11)T6 and occurs only when there are more than 900 H.323 voice calls.

  Workaround: Do not enter the **show voice call status** command in a stress situation.

- CSCsc21446

  Symptoms: Multiple Internet Key Exchange (IKE) security associations (SAs) are created.

  Conditions: This happens only in case of EzVPN configuration.

  Workaround: There is no workaround.

- CSCsc21674

  Symptoms: PSTN is sending in an "*" and the router is reading it in as a ìDî. PSTN is also sending in a "#" and router is reading it in as an "*".

  Conditions: This symptom has been observed on an MGCP T1-CAS gateway connected to Cisco CallManager doing MF and using Cisco IOS Release 12.3.8.T11, Release 12.3.11.T7, or Release 12.3.14.T4..

  Workaround: There is no workaround.

- CSCsc22043

  Symptoms: The TCL script feature on Cisco IOS routers allows the use of CLI commands to be issued and the response to be checked for certain matching conditions. When using the TCL script with the **cli_open** command, a VTY for that script is setup for the exec commands to be issued. The output to the VTY only catches (with the **cli_read** and **cli_read_pattern** commands) output which is directly printed out as a result of the command; i.e., allows the script to match the output of the **show interface** command.

  Output as the results of debug and syslog cannot be seen by the script. Some test commands on the gateway also uses debug to display the output and this can cause problems trying to monitor for certain conditions.

  Conditions: This symptom has been observed by using TCL script to monitor the output of syslog or debug output on the VTY session which the script is using.

  Workaround: There is no workaround.

- CSCsc22552

  Symptoms: Low address access is reloaded at address 0xC when attempting to use a TCL script.

  Conditions: When using the Cisco IOS TCL script feature, if the available processor memory is not enough for the amount required by the TCL script while executing, the IOS router may unexpectedly reload. Caution should be used when using certain TCL script commands which may need a large block of memory. For example, using **cli_exec** commands for a **show** command output which is very large may lead into this problem if the router is running low on processor memory.

  Workaround: Change the TCL script to minimize the impact of memory being used. For example, instead of a **cli_exec** command which buffers the results of the command, try the **cli_write** command and redirect the output of the **show** command off to a location where the output can be stored.

- 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.

- CSCsc27337

  Symptoms: A Cisco router may reload with a bus error.

  Conditions: This symptom has been observed when IPS is enabled with the MSN Messenger Client DNS Request signature or Yahoo Messenger Client DNS Request signature.

  Workaround: Delete the MSN Messenger Client DNS Request or Yahoo Messenger Client DNS Request signature with the **ip ips signature** *sig-id* **delete** command.

- CSCsc27474

  Symptoms: The **show ip mcache** command output would not display the MAC header on a multicast Multilink Frame Relay (MLFR) router.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(5).

  Workaround: There is no workaround.

- CSCsc31082

  Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

  The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in **show frame-relay pvc** show the packets correctly.

  Conditions: A map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

  Workaround: There is no workaround.

- CSCsc39557

  Symptoms: Spurrious memory access errors are encountered that may cause a bus error crash.

  Conditions: This symptom is observed on a Cisco 2800 router that is utilizing voice and is running Cisco IOS Release 12.4(3). This appears to be seen only when caller-id is enabled on FXS ports.

  Workaround: Disable caller-id on any FXS ports.

- CSCsc40912

  Symptoms: SNA Switch (SNASw) routers experience a software-forced crash. The following message is seen in the log:

  ```
  validblock_diagnose, code = 1
  ```

  Conditions: This symptom has been observed after issuing an **inact giveback** command at VTAM directed at the router:

  V NET,INACT,ID=dlurname,GIVEBACK,FINAL=YES

  where *dlurname* is the router CP name.

This symptom occurs during VTAM VARY INACT GIVEBACK processing. This is a regression problem caused by CSCsb11554 so it is only applicable if running Cisco IOS after Cisco IOS interim Release 12.3(15.8), Release 12.4(2.11) and Release 12.4(2.11)T.

Workaround: There is no workaround.

- CSCsc41913

  Symptoms: A Cisco IOS gateway using Cisco IOS Release 12.3(8)T or later versions will use an ephemeral port to send a response to any SIP request. This may not work with port restricted NAT, which is expecting a response on the same connection as the one on which the request was sent and may drop the response.

  Conditions: This symptom is observed on a Cisco IOS gateway with Cisco IOS Release 12.3(8)T or later releases and a port restricted NAT.

  Workaround: There is no workaround.

- CSCsc42335

  Symptoms: Tunneled packets that terminate on a device with an SII intercept in place do not get intercepted.

  Conditions: This symptom occurs if the device on which the tunnel terminates has SII intercepts that match the inner packet. SII will not intercept the packet.

  Workaround: If the packets to be intercepted must arrive via a tunnel, there is no workaround. If not, another method of transport will allow the packets to be intercepted.

- CSCsc42938

  Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured globally or on an interface.

  Conditions: This symptom is observed when you enter the **show mpls ldp neighbor** command while LDP sessions are coming up or going down.

  Workaround: There is no workaround.

- CSCsc44237

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

  The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

  Condition 1: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646 and http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831.

  Cisco IOS software releases that are not listed in the "First Fixed-in Version" fields at these locations are not affected.

  Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

Condition 2: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf** *vrf-name* command is configured, enter the **ip vrf forwarding** *vrf-name* command on at least one interface that has PIM enabled.

- CSCsc44660

  Symptoms: A software-forced crash may happen with following messages:

```
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer at
10.10.10.10
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 10.10.10.10  failed its sanity
check or is malformed
%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
            destaddr=10.20.10.10 prot=50, spi=0x6943127C(1766003324),
srcaddr=10.10.10.10
```

  Conditions: This symptom has been observed when using Internet Security Association and Key Management Protocol (ISAKMP) with over 100 different ISAKMP policies.

  Workaround: Reduce the number of configured ISAKMP policies.

  Further Problem Description: If a router is affected by this software detect, the issue seems to happen around 24hours after reloading the router.

- CSCsc44856

  Symptoms: After HCCP switchover, CEF may have adjfibs in the wrong VRF and incomplete adjacencies.

  Conditions: This symptom occurs on a Cisco uBR10000 router with cable modem interface redundancy that is switching over from a subinterface in one VRF to an interface in a different VRF.

  Workaround: There is no workaround.

- CSCsc48543

  Symptoms: A Cisco router crashes when the E3 controller is shutdown using SNMP.

  Conditions: This symptom is observed on a Cisco 7200 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCsc51183

  Symptoms: A Cisco AS5850 may restart because of a software forced crash preceded by the following error:

```
%SYS-6-STACKLOW: Stack for process VTSP running low, 0/12000
```

Conditions: This symptom has been observed on Cisco IOS Release 12.3(11)T.

Workaround: There is no workaround.

- CSCsc54584

  Symptoms: A standard ingress ACL for transit traffic does not function on an interface that is configured for MFR.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(11)T8 and that has an MFR bundle that is configured on a PA-MC-8TE1 port adapter. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsc64530

  Symptoms: A Cisco 3745 router does not boot up when booting a Cisco IOS with the fix of CSCec74317.

  Conditions: The nvram in the router should be in corrupted state.

  Workaround: Turn the router off and then back on one time will resolve the issue.

- CSCsc64985

  Symptoms: Whenever a voice call is completed, some errant informational messages are echoed to the console and any open Telnet sessions, even though no debugs are enabled. For example, for a DSPless POTS-to-POTS hairpin call, we might see:

```
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  PAK_SUPRESS
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  NSE_PAYLOAD
Nov 30 00:10:37.809 EST:                  SEQ_NUM_START
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  NSE_PAYLOAD
Nov 30 00:10:37.809 EST:                  SEQ_NUM_START
```

  Conditions: This behavior is observed on any Cisco IOS voice gateway which is running a Cisco IOS version listed or implied by the "First Fixed-in Version" field of bug ID CSCsc12570 "mgcp does not switch codec (e.g. g711 to g729) during call".

  Workaround: Use a build of Cisco IOS earlier than those listed or implied by the "First Fixed-in Version" field of bug ID CSCsc12570 "mgcp does not switch codec (e.g. g711 to g729) during call".

- CSCsc66658

  Symptoms: Ping does not work if loopback is configured on the interface.

  Conditions: This symptom has been observed when loopback is configured.

  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.

- CSCsc74783

  Symptoms: Intrusion Prevention System (IPS) signatures that require inspection of TCP flows below port 550 may not be triggered on a Cisco IOS IPS device.

  Conditions: This symptom is observed on a Cisco IOS router that is configured for IPS functionality.

  Workarounds: Apply CBAC (Context Based Access Control) in addition to IPS.

  Further Information: On a Cisco IOS router with IPS (Intrusion Prevention System) enabled, all TCP flows should be subject to TCP stateful inspection until the TCP 3-way handshake is complete. This does not work for TCP sessions with a destination port that is less than 550, if it does not match a predefined signature on the router.

- CSCsc80794

  Symptoms: 100% CPU utilization will be observed on Cisco 2811, Cisco 2821, and Cisco 2851 routers even with no or minimal traffic.

  Conditions: This will happen on the Cisco 2811, Cisco 2821, and Cisco 2851 routers with the images that have integrated the CSCsc10961 fix and have Serial, or DSL interfaces on the native HWIC slots.

  Workaround: There is no workaround.

- CSCuk59798

  Symptoms: The router crashes on removal of a Virtual-TokenRing subinterface. The router also crashes on removal of a main Virtual-TokenRing interface when that main interface also has subinterfaces configured.

  Conditions: This symptom has been observed under the following conditions: 1. Create a main Virtual-Tokenring interface. 2. Create a Virtual-TokenRing subinterface on the interface created in step 1. 3. Remove either the Virtual-TokenRing main interface created in step 1, or the Virtual-TokenRing subinterface created in step 2.

  Workaround: There is no workaround.

Protocol Translation

- CSCei15942

  Symptoms: You may not be able to download a complete file from an FTP during a V.120 session.

  Conditions: This symptom is observed on a Cisco AS5400 and Cisco AS5850 that runs Cisco IOS Release 12.2(15)ZK6 or Release 12.3(11)T5. The symptom could also occur in other releases such as Release 12.3 or Release 12.4.

  Workaround: This problem can be circumvented by disabling the negotiation of multilink on the client adapter or the router. Alternatively, configuring **ppp multilink queue depth fifo 10** on the Virtual-Template interface should allow for a successful FTP download.

TCP/IP Host-Mode Services

- CSCsb51019

  Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state and the following error message is generated:

  ```
  %TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
  ```

Conditions: This symptom is observed on a Cisco 12000 series that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco 12000 series.

Workaround: Identify the BGP connection which is staled with the command **sh tcp brie** and then clear the TCP contol block with the command **clear tcp tcb** *tcb_number* to delete the stuck BGP connection.

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

  Further Problem Description: BGP in Cisco IOS Release 12.0S and Release 12.4 is not affected because the retransmit timeout is disabled for BGP in these releases.

Wide-Area Networking

- CSCed52110

  Symptoms: IP header compression does not function for FR PVC-Bundles.

  Conditions: This symptom is observed when IP header compression is configured for Frame Relay PVC bundles.

  Workaround: There is no workaround.

- CSCee75882

  Symptoms: A GEIP+ may crash unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series when the Gigabit Ethernet interface is transmitting a large amount of traffic and the tx_ring fills up.

  Workaround: Reduce traffic load.

- CSCeg77994

  Symptoms: A LAC does not send an Accounting-Start RADIUS record to a RADIUS server for a user session.

  Conditions: This symptom is observed on a Cisco platform that functions as a LAC and that runs Cisco IOS Release 12.3(14)T1 when a switchover occurs from one LNS to another LNS while the user session is brought up.

  Workaround: There is no workaround.

- CSCeh58376

  Symptoms: A serial interface on a channelized port adapter may stop forwarding traffic through the router but traffic to and from the router over the interface may still go through. The Tx accumulator "value" counter in the output of the **show controllers cbus** Exec command does not exceed the value 2, as is shown in the following example:

```
Router#sh controllers cbus | include
Serial5/1/0.1/2/6/2:0
Serial5/1/0.1/2/6/2:0, txq E8001B40, txacc E8000412 (value 2), txlimit 26
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when QoS is configured on at least one interface on the VIP in which the channelized port adapter is installed. The symptom occurs after the affected interface has flapped very frequently because of OSI layer 1 errors.

Workaround: Remove and reconfigure the controller of the affected interface.

- CSCei94893

  Symptoms: AToM PVCs on an MFR interface that has keepalives disabled do not pass traffic after the router is rebooted.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S.

  Workaround: Enable LMI keepalives.

- CSCej07422

  Symptoms: A Cisco1700 router might unexpectedly crash after entering the **clear pppoe all** command.

  Conditions: This symptom occurs only when PPPoE/IPSec is configured with GRE on the same interface.

  Workaround: Do not configure GRE with PPPoE on the same interface. The functionality of passing packets with GRE configured is not supported.

- CSCej31330

  Symptoms: If predictive LCP negotiations are enabled on a Point-to-Point Protocol (PPP) interface, various problems may arise if negotiations do not proceed as the mechanism predicts. These problems can include the router crashing.

  Conditions: A known situation is that the router may crash with an address error or invalid program counter, accessing address 0x0B0D0B0D, if predictive LCP is enabled on interfaces which negotiate to use Multilink PPP. Other failures may occur.

  Workaround: Disable predictive negotiations (remove "ppp lcp predictive" from the configuration).

- CSCej45061

  Symptoms: Attempts to remove a PRI group fail.

  Conditions: This symptom is observed when an NFAS group has group number 0 and when you attempt to remove a FAS PRI group.

  Workaround: Shut down the NFAS group before you remove the FAS PRI group.

- CSCej45787

  Symptoms: A Cisco 10000 router acting as a PPPoE over ATM server could get crash.

  Conditions: This symptom has been observed when:

  1. PPPoE is running over ATM media. The symptom has not been observed with PPPoE protocol running over Ethernet media.
  2. Dynamic Bandwith Selection feature is enabled. This crash is rarely experienced when DBS feature is not enabled.
  3. These conditions exist on Cisco 10000 routers.

  Workaround: There is no workaround.

- CSCej73049

  Symptoms: AAA method may fail on calls in the Cisco IOS 12.3(11)T releases.

  Conditions: This symptom was observed on a Cisco AS5850 that was running Cisco IOS Release 12.3(11)T8 but is not platform dependent.

  Workaround: There is no workaround.

- CSCsb83234

  Symptoms: UDP port 1701 (L2TP) is still opened by a port scan. The router does not send a "port unreachable" message for a packet that uses UDP 1701.

  Conditions: This symptom is observed on a Cisco 1812 router with Cisco IOS Release 12.3(14)YT or Release 12.4(2)T1.

  Workaround: There is no workaround.

- CSCsb89292

  Symptoms: ISDN NFAS failover issues are observed in Cisco IOS Release 12.3(11) T7. If the primary NFAS d-channel is bounced, the switch sees some of the b- channels in "remote busy" (RMB).

  Conditions: This symptom only happens when the primary NFAS d-channel is bounced.

  Workaround: There is no workaround.

- CSCsc01579

  Symptoms: A Cisco 3825 router may crash due to bus error.

  Conditions: This symptom has been observe to occur every couple of hours on a Cisco 3825 router running Cisco IOS Release 12.3(11)T7.

  Workaround: There is no workaround.

- CSCsc07033

  Symptoms: The status of an ATM VC becomes "INAC" after DBS QoS RADIUS attributes are applied.

  Conditions: If DBS QoS RADIUS attributes specified are above the usable line bandwidth of an ATM link, the status of the VC they are applied to will become "INAC".

  Workaround: Don’t specify DBS QoS RADIUS attributes (atm:peak-cell-rate, atm:sustainable-cell-rate) that are above the usable line bandwidth (149760 for an OC3 ATM link).

- 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.

- CSCsc17673

  Symptoms: Using the **show caller full** or **show caller interface Virtual-Access XX full** commands on a PPPoE client interface causes the router to unexpectedly reload.

  Conditions: This symptom has been observed on routers using Cisco IOS Release 12.4(3.3) and later versions.

  Workaround: Avoid using those commands.

- CSCsc25964

  Symptoms: A PPPoE client router does not honor the **ip mtu** settings configured on the PPPoE Dialer interface when the IP MTU is different from the interface MTU.

  Fragmentation of IP packets larger than the configured IP MTU will not happen which can create problems in a PPPoE environment.

  Conditions: This symptom occurs whenever a vaccess is cloned from the dialer interface and could be PPPoE, multilink or PPPoA.

  Workaround: Configure the **interface mtu** command to the required value.

- CSCsc30497

  Symptoms: NAS-Port Pre-Auth failure breaks PPPoE session limit per VLAN. Once the authorization fails, local limit does not get applied to a particular interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.3YM.

  Workaround: There is no workaround.

- CSCsc33439

  Symptoms: A virtual-access interface fails to come up after you have configured virtual templates.

  Conditions: This symptom is observed on a Cisco router that is configured for MFR.

  Workaround: There is no workaround.

- CSCsc34911

  Symptoms: After applying a RADIUS DBS UBR QoS to an ATM virtual circuit (VC), the QoS becomes QoS VBR, with an SCR of 1, instead of QoS UBR.

  Conditions: This symptom has been observed when specifying a RADIUS DBS QoS UBR and applying it to an ATM VC.

  Workaround: There is no workaround.

- CSCsc49637

  Symptoms: If a PPPoE client session is timed out (e.g. due to a network outage), and a restart of the session is subsequently unsuccessful (e.g. because network outage persists or the PPPoE server has not timed out the prior session) and if the user then manually clears the session, then the router will no longer be able to bring up this session until a reload is performed.

  Conditions: This symptom has been observed when the PPPoE session is unexpectedly interrupted with Cisco IOS Release 12.3(8)T8 or Release 12.3(11) T5. The next feature also needs to be configured.

  ```
  pppoe-client dial-pool-number 1 dial-on-demand
  ```

  Workaround: Use the following procedure:

  1. Reload.
  2. Do not configure the DDR feature for the PPPoE session. This problem is limited to PPPoE client sessions using the DDR feature.

- CSCsc59584

  Symptoms: Cisco IOS Release 12.4(3) and Release 12.4(5) GROUP SERVICE messages are not correct to the PGW.

  Conditions: The following actions will result in all circuits on the PGW to remain in MATE_UNAVAIL state.

  1. Set the IUA destination to out of service (OOS) and then set it to in- service.

2. Set the IUA association to out of service (OOS) and then set it to in- service.
3. Restart the PGW.

Workaround: Reload the IUA to clear the circuits.This is unacceptable to a live customer.

Resolved Caveats—Cisco IOS Release 12.4(5c)

Cisco IOS Release 12.4(5c) is a rebuild release for Cisco IOS Release 12.4(5). The caveats in this section are resolved in Cisco IOS Release 12.4(5c) but may be open in previous Cisco IOS releases.

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.

- CSCej30903

  Symptoms: A router allows logging into the root (or any other configured) view without prompting for a password.

  Conditions: This symptom is observed when no method list is configured for login service.

  Workaround: Configure a method list for the login service.

- CSCek33076

  Symptoms: A RADIUS progress code is incorrectly reported for a call that fails at IPCP. The progress code reports that the Link Control Protocol (LCP) is the open state.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(3a) and that is configured for AAA. The symptom is not release-specific.

  Workaround: There is no workaround.

- CSCek40060

  Symptoms: RADIUS server authentication may not function for dialup and PPP clients.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) and that has the **radius-server retry method round-robin** command enabled.

  Workaround: Disable the **radius-server retry method round-robin** command. Note that the symptom does not occur in Release 12.3 or Release 12.3T.

- CSCin99788

  Symptoms: An “%AAA-3-ACCT_LOW_MEM_TRASH” error message is generated when a low-memory condition occurs. When this situation occurs, a memory leak may occur in AAA data.

  Conditions: This symptom is observed when an interface flaps and causes a very large number of sessions to go down simultaneously, in turn generating a very large number of accounting stop records. In this situation, the I/O memory may be held for a long time when accounting records are send and when an AAA server is slow or unreachable.

  Workaround: There is no workaround.

- CSCir00074

  Symptoms: A router crashes when the casnDisconnect object is set to “true” for a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series when you attempt to terminate the PPPoE session through SNMP by using the casnDisconnect object of the CISCO-AAA-SESSION-MIB.

  Workaround: There is no workaround.

- CSCsa43465

  Symptoms: Users may be able to access root view mode (privilege level) 15 without entering a password.

  Conditions: This symptom is observed on a Cisco router that has the Role-Based CLI Access feature enabled and occurs when the **none** keyword is enabled in the default login method list.

  For example, the symptom may occur when you enter the **aaa authentication login default group tacacs+ none**. When the TACACS+ server is down, users are allowed to enter non-privileged mode. However, users can also access the root view through the **enable view** command without having to enter a password.

  Workaround: Ensure that the **none** keyword is not part of the default login method list.

  Further Problem Description: The fix for this caveat places the authentication of the **enable view** command in the default login method list.

- CSCsb43767

  Symptoms: RADIUS stop packets that are sent to a RADIUS server may contain an incorrect value for the NAS-Port attribute (RADIUS IETF attribute 5). Information that is related to the asynchronous interface is not included in the Cisco-NAS-port VSA.

  Conditions: This symptom is observed on when a Cisco router sends stop packets to a RADIUS server via an asynchronous interface.

  Workaround: There is no workaround.

- CSCsc27615

  Symptoms: RSP QAERROR is seen with a VIP crash and MEMD carve due to standby OIR or another VIP crash at close intervals.

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

  Workaround: There is no workaround.

- 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

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

Workaround: There is no workaround.

- CSCse49728

  Symptoms: SNMPv3 informs are not sent out after a device reload.

  Conditions: This symptom is observed when SNMPv3 informs have been configured, and the device is reloaded.

  Workaround: Re-enter any of the **snmp-server host** commands.

- CSCsf19139

  Symptoms: %RADIUS-3-NOSERVERS messages are logged after a reload in Cisco IOS Release 12.3(18). At this time, the RADIUS accounting tickets are not generated.

  Conditions: This symptom has been observed on a Cisco AS5300 gateway.

  Workaround: Enter into configuration mode and change the order of the servers under the server group.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

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

Interfaces and Bridging

- CSCsc66187

  Symptoms: Error messages such as the following one may be generated on a Cisco router:

  ```
  %CWPA-3-IPCALLOCFAIL: Failed to allocate IPC buffer for loveletter data
  ```

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured with a 1-port Packet-over-SONNET OC-3c/STM-1 multimode port adapter (PA-POS-OC3MM) when you enter the command **no shutdown** on an interface.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- CSCed84633

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

  Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206. 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 fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCek32244

  Symptoms: Not all classful networks are locally generated in the BGP table.

  Conditions: This symptom is observed on a Cisco router that has the **auto-summary** command enabled and occurs when classful networks are provided before the routes are made available in the routing table.

  Workaround: There is no workaround.

- CSCek47667

  Symptoms: A router may not clear BGP routes when you enter the **clear bgp ipv6 unicast *** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SXF but is not release-specific.

  Workaround: There is no workaround.

- CSCsc49231

  Symptoms: The following traceback may appear when NHRP is configured:

  ```
  Nov  5 00:50:41 UTC: %SYS-3-MGDTIMER: Running timer, init, timer = 46D8D2AC.
  -Process= "NHRP", ipl= 0, pid= 226
  -Traceback= 0x41250D34 0x42329F94 0x4232A0D8 0x4232A2E8 0x426A6434 0x426A9424
  0x41CB67D8 0x41CB7A5C 0x41CB8C8C 0x41CB8DF4 0x41CBA394
  ```

  Condition: This symptom has been observe when NHRP is configured.

Workaround: There is no workaround.

- CSCsd33445

  Symptoms: A Cisco platform that is configured for Next Hop Resolution Protocol (NHRP) may display an error message similar to the following:

  ```
  %SYS-3-MGDTIMER: Running timer, init, timer = 0xXXXXXXXX Process= "NHRP", ipl= 0, pid=
  YYY
  ```

  Conditions: This symptom is observed in a DMVPN environment.

  Workaround: There is no workaround.

- CSCse29428

  Symptoms: A crash is seen with %ALIGN-1-FATAL after showing %SYS-2-CHUNKEXPANDFAIL and %SYS-2-MALLOCFAIL repeatedly.

  Conditions: This symptom is observed on a Cisco 3725 router that is running Cisco IOS Release 12.4(5a) with the c3725-advipservicesk9-mz image that is running IPSec VPN.

  Workaround: There is no workaround.

- CSCse64256

  Symptoms: When a First Hop Router receives (S,G) stream for an Embedded RP group, the router crashes while trying to send register packets.

  Conditions: This symptom has been observed on a First Hop Router.

  Workaround: There is no workaround.

- CSCse98590

  Symptoms: The router will display SYS-2-MALLOCFAIL messages on the console, and various protocols will operate erratically as a result of a low memory condition.

  Conditions: When a router has to duplicate incoming IPv4 multicast packets for transmission on multiple interfaces, and one of those interfaces is a GRE tunnel operating in GRE IPv6 mode, then memory used to duplicate that packet stream will not be freed. As a result, the router will soon exhaust all available memory.

  Workaround: The router will not exhaust memory if packets do not need to be duplicated (for example, if they enter on one interface and only exit the box through another interface), or if they do not need to duplicate to a tunnel interface that is running GRE over IPv6 (for example, tunnel mode GRE IPv4 does not have this problem).

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Condition: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh80678

  Symptoms: New or flapping IGP routes may be injected into BGP even though no corresponding network statements exist.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(22) or a later release when the **auto-summary** command is enabled for BGP.

  Workaround: Enter the **no auto-summary** command.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

  Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  Workaround: Add area 0 in the OSPF VRF processes.

  Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

- CSCuk58462

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- CSCsb07279

  Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

  Conditions: Normal operation.

  Workaround: To have a change take effect immediately, enter the **no redistribute route-map** command followed by the **redistribute route-map** command for the IS-IS router process.

- CSCuk60585

  Symptoms: If redistribution into ISO-IGRP is configured, a crash may occur if the router configuration is then nv-gened.

  Conditions: This symptom is observed when redistribution into ISO-IGRP is configured.

  Workaround: If you do not redistribute into ISO-IGRP the bug will not occur. Deconfiguring such distribution means the bug will not occur. Deconfiguring before nv-genning the router's configuration will mean that the bug does not occur.

Miscellaneous

- CSCds25257

  Symptoms: A gatekeeper rejects new registration requests from a Cisco Unified CallManager (CUCM) or other H.323 endpoints with Registration Rejection (RRJ) reason of duplicateAlias. Attempting to clear this stale registration fails and a “No such local endpoint is registered, clear failed.” error message is generated.

  Conditions: This symptom is observed in the following topology:

  CUCM H.225 trunks register to a gatekeeper (GK) cluster. Gatekeeper 1 (GK1) and gatekeeper 2 (GK2) are members of the GK cluster. The CUCM registers first to GK1, then fails over to GK2. This registration at GK2 sends an alternate registration to GK1. However, because of network issues, the unregistered indication does not reach GK1.

  When the H.225 trunk attempts to register with GK1, it is rejected because the alternate registration is still present, and there is no way to clear it.

```
10.9.20.3       34273 10.9.20.3       32853 SJC-LMPVA-GK-1    H323-GW A
    ENDPOINT-ID: 450FC24400000000  VERSION: 5  AGE: 1618993 secs
SupportsAnnexE: FALSE
    g_supp_prots: 0x00000050
    H323-ID: SJC-LMPVA-Trunk_4
```

  Workaround: Reset the gatekeeper by entering the **shutdown** command followed by the **no shutdown** command, or reboot the affected GK.

- CSCef29090

  Symptoms: The throughput for TCPClear sessions on a Cisco AS5850 may not be as expected and there may be a slow response time.

  Conditions: This symptom is observed on a Cisco AS5850 with TCPclear sessions.

  Workaround: There is no workaround.

- CSCek24468

  Symptoms: Dangling bearer channels or voice DSP channels may occur.

  Conditions: This symptom is observed under heavy stress with short duration calls on a Cisco platform such as a Cisco AS5400 or Cisco AS5850 that functions as a gateway.

  Workaround: There are no workaround.

- CSCek34049

  Symptoms: A Cisco AS5850 that is configured for RPR+ may be unable to process more than 1990 MGCP voice calls. With more than 1990 MGCP voice calls, any of the following symptoms may occur:

  - Many DSP may time-out.
  - Active calls may hang.
  - Spurious memory accesses and tracebacks may be generated.
  - Incoming calls may be dropped.
  - NextPort SPE ports may be stuck in the “a” state.

  Conditions: These symptoms are observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(3d) or Release 12.4(7a).

Workaround: There is no workaround. A Cisco AS5850 that is used to its full capacity (4 CT3 worth of MGCP calls) may not scale beyond 1990 calls. When the symptoms have occurred, reload the Cisco AS5850.

- CSCek37686

  Symptoms: A Cisco AS5350 may reload because of a bus error (SIG=10).

  Conditions: This symptom is observed when SNMP is configured and when SNMP queries are made into the Cisco AS5350.

  Workaround: Disable SNMP or stop polling the router.

- CSCek38136

  Symptoms: When you deploy VoIP using PVDM2 / 5510 DSP modules, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with 5510 DSP modules. The symptom does not occur with 549 DSP modules.

  Workaround: There is no workaround.

- CSCek42816

  Symptoms: A voice gateway reloads while bulk calls are being processed.

  Conditions: The symptom is observed on a Cisco voice gateway that runs VXML applications that stream voice when the voice gateway receives prompts from an HTTP server.

  Workaround: Enter the **ivr prompt streamed none** command on the voice gateway.

- CSCin99565

  Symptoms: A router that is configured for SSG may reload unexpectedly.

  Conditions: This symptom is observed when both the Transparent Auto-Logon (TAL) and Port-Bundle Host-Key (PBHK) SSG features are enabled and when it takes a long time before the AAA server responds.

  Workaround: There is no workaround.

- CSCsa70712

  Symptoms: When you reload a CMM in one slot, the CMM in another slot reloads too, and the console of the supervisor engine shows an “EarlRecoveryPatch Reset” error message for the CMM that you intentionally reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series when you enter the **reload** command via the console of the CMM.

  Workaround: Do not reload the CMM via its console. Rather, enter the **hw-module module** *slot number* **reset** command for the CMM on the supervisor engine.

- CSCsb23038

  Symptoms: While attempting performance/stress testing, a memory leak is experienced. The Terminating Gateway (TGW) could not be accessed through the console, the following message was output:

  ```
  %% Low on memory; try again later.
  ```

  The root cause is that the calls are being hung. SIP KPML was enabled on half of the dial-peers.

  Conditions: This symptom is observed on a Cisco 3700 series router.

  Workaround: Do not enable DTMF Relay on the dial peers, for example SIP KPML and others under heavy load conditions.

- CSCsb93407

  Symptoms: When H323 call service stops, the router still listens on TCP port 1720 and completes connection attempts.

  Conditions: This symptom occurs after H323 is disabled using the following configuration commands:

  voice service voip h323 call service stop

  Workaround: Access can be blocked by deploying an interface access list that blocks access to TCP port 1720 for traffic that is destined for any of the IP addresses of the router.

  For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document at http://www.cisco.com/warp/public/707/tacl.html

  For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document at http://www.cisco.com/warp/public/707/iacl.html.

  For information about using control plane policing to block access to TCP port 1720, see the "Deploying Control Plane Policing White Paper" at http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a .shtml.

- CSCsc12255

  Symptoms: When you deploy VoIP on an NM-HDV2 network module that is configured with a PVDM2-64 module, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with an NM-HDV2 network module. Note that the symptom does not occur with an NM-HDV network module.

  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.

- CSCsc95234

  Symptoms: When the **stcapp** global configuration command is enabled, the command is not accepted and the following error messages are generated:

  ```
  STCAPP: Internal error: Unable to create codec list... exiting
     stcapp shutdown initiated... waiting for calls to clear.
     stcapp shutdown complete.
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(6.3) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCsc97398

  Symptoms: The user information Layer 1 protocol may be included in the outgoing bearer capability and may be set to either G711 u-law or G711 A-law. Some PBXs may refuse the call because of this mismatch in the bearer capability.

  Conditions: This symptom is observed when a call is made from H.323 to ISDN with unrestricted digital information bearer capability.

  Workaround: There is no workaround.

- CSCsd11811

  Symptoms: A Cisco 1760 router that is running Cisco IOS Release 12.4(6.7) may reload due to a software-forced crash.

  Conditions: The trigger is due to improper packet cleanup when the buffer allocation fails under high CPU load.

  Workaround: There is no workaround.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that runs Cisco IOS Release 12.4(3b)B. The router has services 81, 82 and 90 configured. The only service that has a problem is 90. The packet traces indicate that the router is sometimes responding to "Here_I_Am" messages from the cache with "I_See_You" messages that contain an incorrect destination IP address. This situation leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3b) but may also affect other releases.

  Workaround: There is no workaround.

- CSCsd28214

  Symptoms: A Cisco router may crash because of a watch dog timeout while running the RIP routing protocol.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3(19) when an interface changes state at the exact same time that a RIP route that was learned on this interface is being replaced with a better metric redistributed route. For example, when RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0 interface and then RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, the RIP route is removed. However, when during this time the Fast Ethernet 1/0 interface goes down, the router may crash because of a watch dog timeout. Note that the symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCsd35389

  Symptoms: When a Cisco Unified CallManager Express (Cisco Unified CME) registers with a gatekeeper, all the ephone-dns are automatically registered. When an ephone-dn is deleted, it does not unregister with the gatekeeper. If you enter the **no gateway** command followed by the **gateway** command on the CME router to force it to unregister then reregister, the deleted ephone-dn will show up again.

  Conditions: This symptom is observed on a Cisco 3800 series router.

  Workaround: To permanently remove the ephone-dn reload the CME/gateway or enter the **shut** command followed by the **no shut** command on the gatekeeper.

- CSCsd37629

  Symptoms: Alignment errors and a bus error may occur on a Cisco platform that has the **ip inspect** command enabled.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: Disable the **ip inspect** command.

- CSCsd44118

  Symptoms: When running TCL/VXML applications that perform Media Play, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: This symptom is observed when Cisco IOS Media Play code forgets to release a memory at the end of Media Play.

  Workaround: There is no workaround. Contact Multiservices TAC (IOS) and request a patch.

- CSCsd66800

  Symptoms: A gateway-controlled T.38 fax relay between an MGCP gateway and another gateway may be disconnected unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that is configured for Voice xGCP.

  Workaround: There is no workaround.

- CSCsd73526

  Symptoms: When a Cisco Content Services Switch (CSS) is used in a Customer Voice Portal (CVP) configuration, the Cisco IOS Voice Browser may be unable to play the media file. The CSS does send the HTTP Redirect message that points to the CVP, but the gateway does not react.

  Conditions: This symptom is observed on a Cisco AS5400HPX Universal Gateway after you have upgraded this platform from Cisco IOS Release 12.3(3a) to Release 12.4(3b). Other software components in the configuration are CVP 3.1 SR1, ICM 6.0, and Cisco CallManager 4.1(3)SR2.

  Workaround: Bypass the Cisco CSS, and point the VXML application directly to the CVP.

- CSCsd76444

  Symptoms: A Cisco router may reload unexpectedly with a “Signal 0” without a stack trace in the crash info file.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE and that is configured for SSG. However, the symptom is platform-independent and may occur on any router that is configured for SSG.

  Workaround: There is no workaround.

- CSCsd79558

  Symptoms: When tunnel protection is configured on a tunnel interface, an IPSec session may fail to come up.

  Conditions: This symptom is observed when the **tunnel vrf** *vrf-name* command is changed on the tunnel interface.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove and re-add the tunnel interface.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  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.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM) CSCsi97695

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

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

Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle. shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.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.

- CSCse01847

  Symptoms: When agentless hosts are allowed network access, a loss of connectivity may occur during reauthentication.

  Conditions: This symptom is observed when the host does not have a Cisco Trust Agent (CTA) configured.

  Workaround: There is no workaround.

  Further Problem Description: When an agentless host is authorized for network access, a dynamic access policy is applied for the host. This access policy is removed at the beginning of the reauthentication process, and re-applied at the end of reauthentication process. During the reauthentication process, no access policy is applied for the host. This situation may cause a disruption to network access.

- CSCse03855

  Symptoms: An IP phone display remains stuck at “Enter Number” for the duration of an outgoing call to the PSTN.

  Conditions: This symptom is observed when the IP phone runs CME version 3.3 and is connected to a BRI ISDN interface on a Cisco router that runs Cisco IOS Release 12.4. When you enable the **debug isdn q931** command, the following message is displayed in response to an outgoing setup message:

  ```
  ISDN BR0/2/0 Q931: RX <- SETUP_ACK pd = 8  callref = 0x83
  Channel ID i = 0x89
  Progress Ind i = 0x8288 - In-band info or appropriate now available
  ```

  Workaround: Prevent the Telco from sending the following information in the setup_ack message:

  ```
  Progress Ind i = 0x8288 - In-band" information or appropriate now available
  ```

  Note that the symptom does not occur in Cisco IOS Release 12.3(11)T10 and with CME version 3.2.

- CSCse05642

  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

- CSCse15025

  Symptoms: An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

  When this problem occurs, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

  Because this issue impacts the signaling channels, it has been seen that calls either will not connect at all through impacted ports or in some cases when multiple simultaneous calls are present on adjacent voice ports/timeslots, the call may connect momentarily before being disconnected.

  If a problem occurs only on a single voice port, there is another problem, not this caveat (CSCse15025). PRI/BRI calls are not affected because PRI/BRI does not utilize the DSP for signaling purposes.

  When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port- number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41, and 42 is presented and some of the registers show double- octet information. See the example output (2) below.

  When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** *port- number* **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

  Further Problem Description: The changes in CSCse15025 includes changes in CSCsc11833 and CScsd90851. These changes have been shown to help mitigate this problem in the majority of cases.

  There is a further detection and reset mechanism in CSCse15025 that will recover the DSP which is in this state. This mechanism will trigger immediately if the impacted voice port is an analog FXO port. For other voice ports, a delay in the detection will be present and it is possible to see the symptom of this problem before the recovery code triggers.

  Note that the reset mechanism will cause any active calls utilizing the DSP in question to be dropped.

  It is recommended if running with modules which can be impacted by this issue to upgrade to a release of software which contains the changes in CSCse15025. If the DSP is reset and the below output is seen, contact the TAC for further assistance. Note that this output is sent at debug level and it is recommended to enable either syslog or logging buffered on the gateway.

  Logging buffered on the gateway is enabled through the global command **logging buffered 50000 debug** as an example to set the logging buffered to use 50K bytes of processor memory for logging. The output of the log can be seen with the exec command **show log**.

  Example output when detection and recovery code on gateway triggers:

```
*May 31 14:30:43.343: TDM pointers: 0100 0100 0115 0115. Deltas: 0001 0000.
```

```
*May 31 14:30:43.347: Received alarm indication from dsp(0/1)
0030 0000 0080 0000 0013 4100 2E2E 2F2E 2E2F 6D6F 6475 6C65 732F 7363 6865
6475 6C65 2F64 6562 7567 2E63 2833 3634 2900
*May 31 14:30:43.347: ../../modules/schedule/debug.c(364)

*May 31 14:30:43.347: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to Administrative Shutdown
*May 31 14:30:43.647: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to Administrative Shutdown
*May 31 14:30:43.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to Administrative Shutdown
*May 31 14:30:44.247: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to Administrative Shutdown

*May 31 14:30:48.147: Crash dump CLI may not be configured, not able to get
crash info, slot 0, dsp 1
*May 31 14:30:48.147: DSPDUMP - Recover slot 0 dsp 1
*May 31 14:30:48.147: DSPDUMP - ka sent 0, ka_cnt 51193, skip_ka 103079
*May 31 14:30:50.579: %DSPRM-5-UPDOWN: DSP 1 in slot 0, changed state to up
*May 31 14:30:50.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to up
*May 31 14:30:51.219: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to up
*May 31 14:30:51.371: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to up
*May 31 14:30:51.523: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to up
```

Following are command output examples:

1) Following is an example of normal output for FXO and EVM FXS ports.

For FXO ports, the value is usually 0x01 but for EVM FXS the value can be different. When you run the above-mentioned command, the expected output is that a single octet is displayed and only for register 39. (This command does not work for VIC-4FXS and VIC2-xFXS modules).

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
```

Values read from SiLabs Codec connected to DSP 0, channel 11:

```
------------------------------------------------------------
Register 39 = 0x01
```

2) Following is an example of output for FXO and EVM FXS ports that indicates that the symptom has occurred. Note that the exact output for the register values is different, but when the symptom occurs, different lines with information are displayed as shown below:

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#
```

Values read from SiLabs Codec connected to DSP 0, channel 11:

```
------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF
```

3) Following is an example of normal output for FXS and analog E&M modules. The values that are listed in a normal case may be different, but only four registers of a single octet should be displayed.

Values read from PEB2465 Codec connected to DSP 02 (channel 0):

```
------------------------------------------------------------
```

```
Extended Register Values (XR4..XR1) = 00, CC, 50, 11
```

4) Following is an example of output for FXS and analog E&M modules that indicates that the symptom has occurred.

Values read from PEB2x65 Codec connected to DSP 0, channel 1:

```
------------------------------------------------------------
Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t
  ip ssh version 1
  end
  ```

  Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

  ```
  10.1.1.0/24 is a trusted network that
  is permitted access to the router, all
  other access is denied

  access-list 99 permit 10.1.1.0 0.0.0.255
  access-list 99 deny any

  line vty 0 4
  access-class 99 in
  end
  ```

  Further Problem Description: For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

  http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6350_TSD_Products_Configuration_Guide_Chapter.html

  For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

  http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse34097

  Symptoms: When a voice call is made to one of the busy channels of BRI/PRI port, the call gets rejected and then another call is made to the available port. The call gets connected, and the user hears an annoying hissing sound.

  Conditions: The procedure to recreate this scenario is the following:

  Phone a & b ---OGW --VoIP --TGW(2611) --BRI/PRI --PBX -- phone c & d

  Phone a calls phone c; Phone b calls phone c; Phone b calls phone d;

  Phone d picks up and hears a hissing noise.

  Workaround: There is no workaround.

- CSCse42141

  Symptoms: T38 fax calls fail when they come inbound through DID analog ports. When the **debug h245 asn1** command is enabled, you can see that there is no “OLCAck” returned the fax server.

  Conditions: This symptom is observed only on analog ports. PRI works fine in the same configuration.

  Workaround: Send the fax calls through a PRI.

- CSCse45425

  Symptoms: A VAM2 may reset when it receives a malformed ESP packet, and a “Free Pool stuck” error message may be generated. This situation causes high CPU usage in the encryption process while the software is handling the encryption as opposed to the hardware. Even when the VAM2 recovers, the high CPU usage remains because the software-encrypted tunnels do not fall back to hardware encryption until the SA lifetime expires.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(19) or Release 12.4(7a).

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred and after the VAM2 has recovered, disable software encryption by entering the **no crypto engine software ipsec** command to force the encryption back to the hardware.

- CSCse50887

  Symptoms: MGCP IOS Gateway sees the following:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```
  and then:

  ```
  config term
  router(UNKNOWN-MODE)
  ```
  Or, the **show running-config** command output is only 5 bytes.

  Conditions: This symptom occurs under the following conditions:

  - Use MGCP with the **ccm-manager config** command
  - Have more than 20 MGCP end points (voice ports)
  - Run Cisco IOS 12.3(11)T or later releases
  - Reset device pool from Cisco CallManager

  Workaround: Add the **no ccm-manager config** command.

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- CSCse56660

  Symptoms: Inbound calls to FXO ports on Cisco IOS VoIP gateways connect, but audio is not present.

  Conditions: With **caller-id enable** configured on FXO ports, the call will connect, but no audio is heard. When this occurs, the following error message can be seen at debug level:

  ```
  Jun 20 01:41:15.855: mbrd_e1t1_vic_connect: setup failed
  Jun 20 01:41:15.855: flex_dsprm_tdm_xconn: voice-port(0/0/1), dsp_channel (/0/2/0)
  ```

  Workaround: Disable caller id on the voice-port.

- CSCse63494

  Symptoms: A router that is configured for Real-Time Protocol (RTP) may generate CPUHOG events and a traceback similar to the following:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (951/33),process = VOIP_RTCP.
  -Traceback= 0x60EA5A78 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  ```

  Alternatively, the router may unexpectedly reload and generate the following error message and traceback:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = VOIP_RTCP.
  - Traceback= 0x60EA5A58 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  %Software-forced reload
  Preparing to dump core...
  ```

  Conditions: This symptom is observed on a Cisco router that receives a badly formatted RTP Control Protocol (RTCP) packet.

  Workaround: There is no workaround.

  Further Problem Description: Typically, the badly formatted RTCP packet is produced by a device that does not conform to the RFC 3550 standard.

- 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

- CSCsf03530

  Symptoms: A crash occurs on a router when it receives a message waiting indicator (MWI).

  Conditions: This symptom is observed when unity sends a notify to the gateway (GW), and the GW is suppose to convert to QSIG MWI. The GW crashes while running Cisco IOS Interim 12.4(9.18)T.

Workaround: There is no workaround.

- 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

- CSCsf31178

  Symptoms: HWIC-1GE-SFP may experience an issue where the Gig Ethernet interface is “stuck” in a Line UP/Protocol Down state. While in this state, the interface will not pass traffic. Clearing the interface or manually disabling/enabling will clear the condition. This symptom does not occur when 1000BASE-T SFP is used.

  Conditions: A Loss of Signal (for example, unplugging the cable) may cause the interface to become stuck in a Line UP/Protocol Down state.

  Workaround: Clearing the interface or manually shutting it down, then bringing it back up will clear the problem.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsg05350

  Symptoms: A Cisco platform crashes due to a chunk memory leak and generates the following error messages and tracebacks:

  ```
  %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a reload due to
  Fragmented processor_memory, Free processor_memory = 10402472
  bytes, Largest processor_memory block = 522632 bytes
  ```

  Conditions: This symptom is observed on a Cisco AS5850 when there is a chunk memory leak. However, the symptom is platform-independent and relates to the Distributed Stream Media Processor (DSMP).

  Workaround: There is no workaround.

- CSCsg11718

  Symptoms: A VRF may become stuck in the “Delete Pending” state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- 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

- CSCsg76715

  Symptoms: A device crashes when you delete an ACE that was inserted in the middle of the ACL rather than added at the end of the list.

  Conditions: This symptom is observed when all of the following conditions are present:

- The inserted ACE has a destination prefix length of 0, that is, is has an “any” statement instead of a destination address.
- The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an “any” statement), and the inserted ACE has a lower sequence number than this other ACE.
- The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

Workaround: First, delete the inserted ACE. Then, delete the other ACE with the same SRC prefix length and an destination prefix length that is greater than 0.

Alternate Workaround: Delete the complete ACL.

- CSCsg96319

  Symptoms: When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:***number ip-address* command.

  Conditions: This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhanmt_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  Workaround: Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

  ```
  %MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of [dec] - VRF [chars]
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

  Workaround: There is no workaround.

- CSCsh58082

  Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

  There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

  Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsh75827

  Symptoms: When a router that has the **ssg intercept dhcp** command enabled receives a DHCP packet from a host that has already logged out from a Subscriber Edge Services Manager (SESM), the router may unexpectedly reload because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an SSG with PBHK enabled, when a host has received an IP address that is associated with a service (via the "J" Service-Info attribute), has logged out from the SESM, and then renews its IP address.

Workaround: There is no workaround.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi27540

  Symptoms: A VSI session may become stuck in the "RESYNC_UNDERWAY" state, preventing LVC connections from being set up. This situation is not cleared automatically, and error messages are not flushed, as is shown in the output of the **show controller vsi session** command.

  Conditions: This symptom is observed on a Cisco router that functions as a Label Switch Controller (LSC).

  Workaround: There is no workaround.

- 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

- CSCsi67763

  The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

  http://www.kb.cert.org/vuls/id/739224

  By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco response is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml

- CSCsi84017

  Symptoms: When you reload a Cisco 2600 series, the router may hang.

  Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

  Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third party system.

  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.

Wide-Area Networking

- CSCee75882

  Symptoms: A GEIP+ may crash unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series when the Gigabit Ethernet interface is transmitting a large amount of traffic and the tx_ring fills up.

  Workaround: Reduce traffic load.

- CSCek28604

  Symptoms: A Cisco device may reload ("System returned to ROM") unexpectedly due to a memory leak in the ISDN L2 process.

  Conditions: This symptom is observed on a Cisco device that functions in a call manager-backhaul configuration after running under stress for about 24 hours.

  The output of the **show processes memory**, collected in regular intervals shows a memory leak in the ISDN L2 process. The amount of memory that is held by the ISDN L2 process will be very large and growing.

  Workaround: Enter the **isdn k 1** command on all backhauled serial interfaces.

- CSCek31660

  Symptoms: For VPDN sessions that are established with a LAC, the RADIUS progress code in the Stop record may be different from the RADIUS progress code in the Start record.

  Condition: This symptom is observed on a Cisco platform such as a Cisco AS5400 that runs Cisco IOS Release 12.4.(3a) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCek40618

  Symptoms: A router may crash by address error (load or instruction fetch) exception during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP.

  Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.2SB, 12.3, and 12.4 without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCir00712

  Symptoms: When a LAC receives fragmented data traffic over an L2TP tunnel, the IP layer reassembles the packets and routes them over the wrong interface instead of processing them locally.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel. The symptom is release-independent.

  Workaround: There is no workaround.

- CSCsd19867

  Symptoms: BRI interfaces does not come up when you reload a router. You must enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected BRI interfaces to bring them up.

  Conditions: This symptom is observed when you enter the **no isdn spoofing** command and reload the router.

  Workaround: Disable the **no isdn spoofing** command.

- CSCse79994

  Symptoms: BRI Layer 2 remains in the ESTABLISH_AWAITING_TEI state instead of entering the MULTIPLE_FRAME_ESTABLISHED state.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf96318

  Symptom: QSIG (ISO) call back (ring back) fails between a Cisco 3745 router and a Cisco 1760 router.

  Conditions: The call back fails.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg50202

  Symptoms: When a BRI interface flaps rapidly, ISDN Layer 1 detects a link down state, but Layer 2 and Layer 3 may remain in the active state during the transition. This situation may cause the BRI interface to become stuck, and subsequent incoming and outgoing calls to be rejected.

Conditions: This symptom is observed when a cable is pulled out and put back rapidly.

Workaround: Enter the **clear interface** command on the affected BRI interface.

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

- CSCsi74960

  Symptoms: A router crashes while sending large control packets between client and L2TP Network Server (LNS) in L2TP callback scenario.

  Conditions: This symptom happens with a Cisco 7200 router that is running Cisco IOS interim Release 12.4(13.13)T1.

  Workaround: There is no workaround.

- CSCsj10593

  Symptoms: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(15.6) and that functions as a TGW with all PRI switch types from the user to the network side. The symptom occurs when the **isdn test call interface** *interface-number dialing-string* command is entered at the platform on which the call is initiated, when the originating gateway (OGW) is configured for the National ISDN (primary-ni) switch type, and when the TGW is configured for the NT DMS-100 (primary-dms100) switch type. The symptom may also affect Release 12.4T.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(5b)

Cisco IOS Release 12.4(5b) is a rebuild release for Cisco IOS Release 12.4(5). The caveats in this section are resolved in Cisco IOS Release 12.4(5b) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCej18051

  Symptoms: Terminal window PPP clients may fail with Cisco Access servers.

  Conditions: This symptom has been observed on Cisco AS5400 gateways and Cisco AS5800 servers.

  Workaround: There is no workaround.

- CSCek27271

  Symptoms: The IPSLA test packets returned by the IPSLA responder for the UDP jitter operation have ToS value of 0 instead of the value configured for the operation. Because of this, the two IPSLA UDP jitter operations between same source and responder routers with just the different ToS configurations will report the same round trip time even though the expected values are different.

  Conditions: This symptom has been observed on the routers configured with an IP SLA User Datagram Protocol (UDP) jitter operation with microseconds precision and has the ToS value configured.

  Workaround: There is no workaround.

- CSCsb30875

  Symptoms: Active eRSC on a Cisco AS5850 gateway could hang after RPR+ failover, if the **aaa accounting system** command is configured.

  Conditions: The symptom has been observed under the following conditions:

  4. RPR+ failover occurred.
  5. Console connection window closed & reopened to the newly active eRSC after failover.

  Workaround: There are two workarounds.

  1. The eRSC hang will not happen if no attempt is made to close and reopen the console session with newly active eRSC after failover.
  2. Remove the **aaa accounting system** command from the configuration.

- CSCsc19289

  Symptoms: MC-T1 is disabled and wedged when changing the MTU size on the MC-T1 interface.

  Conditions: This symptom has been observed when dLFIoLL is configured on a Cisco 7500 router and the MTU size on MX-serial interface is changed.

  Workaround: Remove and replace the MC-T1 or micro reload the MC-T1.

- CSCsc70055

  Symptoms: Cisco 7200 routers with traffic-carrying port adapters (PA) may crash when a Graceful OIR is done on the traffic-carrying port adapter.

  Conditions: The following conditions may result in a crash of the Cisco 7200 router:

  1. Graceful OIR must be done.
  2. The PA must be carrying traffic and the symptom occurs mostly with ingress traffic on the PA.

  Workaround: Perform a manual OIR.

- CSCsd10306

  Symptoms: IP SLA packets are dropped in the network. They may also cause a buffer leak on some Cisco routers. Frequency of the problem is very low, less then 1%.

  Conditions: This symptom is observed on IP SLA packets that have an MPLS label applied on the source router.

  Workaround: There is no workaround.

  Further Problem Description: The IP SLA packets in question have a corrupted IP header.

Interfaces and Bridging

- CSCei68284

  Symptoms: POS interfaces may remain in the up/down state after the router has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

  Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

IP Routing Protocols

- CSCeg39601

  Symptoms: The IPv6 multicast RP encapsulation tunnel remains down.

  Conditions: This symptom occurs on the configuration of the **ipv6 pim rp-address** command. The resulting encapsulation tunnel is created but remains always in down state.

  Workaround: There is no workaround.

- CSCej62500

  Symptoms: NAT Stateful forces the router to crash when there is heavy traffic exchanged between two peer SNAT routers. When active routers come back and a DUMP request process occurs at the same time, entries time out all together. This generates a large number of ACK packet exchanges and the actual data structure which stores these ACKs cannot handle this amount.

  Conditions: This symptom has been observed with SNAT Active/Standby configuration using the SNAT UDP option. When the NAT table has a size larger than 10000 entries, all entries of the table time out together. This timeout generates high density of packet exchange due to SNAT flow control mechanism.

  Workaround: There is no workaround.

- CSCek10384

  Symptoms: A Cisco 7200 router that is performing NAT could drop IPSec packets.

  Conditions: This symptom is observed on a Cisco 7200 router that is performing NAT functionality for IPSec transit packets. The router will NAT and forward the Inside to Outside IPSec (ESP) packets, but might drop the return IPSec packets from Outside to Inside.

  Workaround: Disable NAT for IPSec.

- CSCsc59089

  Symptoms: BGP does not advertise all routes to a peer that sends a route-refresh request.

  Conditions: This symptom is observed under the following conditions:

  – The router is in the process of converging all of its peers and has updates ready in the output queue for the peer.

  – The peer sends a route-refresh request to the router. This may occur when the **clear ip bgp * soft in** command is entered on the peer or when a VRF is added to the peer.

  – The router processes the route-refresh request from the peer while the router still has updates in the output queue for the peer.

  In this situation, all of prefixes that are advertised by the unsent updates in the output queue for the peer are lost.

  Workaround: There is no workaround. When the symptom has occurred, enter the **clear ip bgp * soft out** command on the router to force the router to send all updates to its peers.

- CSCsd01824

  Symptoms: Extended NAT entries that are created by outside static NAT translation in a VRF SNAT environment do not age out and remain in the translation table until you enter the **clear** command.

  Conditions: This symptom is observed when the **ip nat outside source static** command is configured in a VRF SNAT environment on a Cisco router that runs Cisco IOS Release 12.4.

  Workaround: If this is an option, use the **ip nat inside source static** command in the VRF SNAT environment.

Miscellaneous

- CSCee72997

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCee69887

  Symptoms: A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the **show clns neighbors** command indicates that a certain system interface remains in the "Init" state indefinitely, although the output of the **show ip interface brief** command shows that this interface is up.

  Conditions: This symptom is observed when a dual SRP ring is configured on three routers that run Cisco IOS Release 12.2S. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeh18306

  Symptoms: On a Cisco 2600-XM series that is configured with an AIM-ATM module, when one PVC is configured for ABR and another PVC is configured for another ATM class, CRC errors occur on the far end of the ATM link of the PVC that is configured for the other ATM class. This situation may occur because the PVC that is configured for ABR sends two RM cells in a row and overwrites some data of the PVC that is configured for the other ATM class

  Conditions: This symptom is observed on a Cisco 2651-XM that runs Cisco IOS Release 12.3 and that is configured with an AIM-ATM module. However, the symptom may not be platform-dependent and may occur on any platform that is configured with an AIM-ATM module.

  Workaround: Do not configure ABR on a PVC.

- CSCeh60551

  Symptoms: Certain malformed client certificates may cause an AP that is running Cisco IOS Release 12.3(2)JA2 or 12.3(4)JA to crash when EAP-TLS is used.

  Workaround: Issue a new client certificate.

- CSCej13460

  Symptoms: The packets are not switched correctly using the Fast Switching with IPSec tunnel protection feature.

  Condition: This symptom has been observed in Cisco IOS Release 12.4(1b) when tunnel protection IPSec is configured and tunnel source interface has Fast- switching (but not CEF) configured.

  Workaround: Use CEF switching.

- CSCej27710

  Symptoms: The voicemail box is not available.

  Conditions: This symptom has been observed when a mailbox is assigned to a phone and someone leaves voice mail.

  Workaround: There is no workaround.

- CSCej83415

  Symptoms: A Cisco IOS gateway might crash while running voice calls.

  Conditions: This symptom is observed under high stress/high CPU where race conditions in Cisco IOS are more likely to occur. These race conditions can result in a MIBS data base corruption or RTP memory corruption resulting in a crash.

  Workaround: There is no workaround.

- CSCej85495

  Symptoms: The Cisco AS5400 reloads unexpectedly with the **show csm modem** command.

  Conditions: This symptom is not service impacting.

  Workarround: There is no workaround.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek17148

  Symptoms: A gateway running CME or SRST may crash.

  Conditions: This symptom has been observed with a Cisco 3825 router running CME with two IP phones and one analog phone attached. This symptom has been observed with both Cisco IOS Release 12.4(4)T and Cisco IOS interim Release 12.4(5.2)T.

  Workaround: There is no workaround.

- 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

- CSCek30748

  Symptoms: A router reloads when you enter the **tunnel protection ipsec profile vpnprof** command.

  Conditions: The symptom can be observed on a Cisco 7200 series but may be platform-independent.

  Workaround: There is no workaround.

- CSCek33253

  Symptoms: NextPort modems that function in a T1 CAS signaling configuration do not dial all the DTMF digits successfully.

  Conditions: This symptom is observed when you enter valid DTMF digits such as # and * in dial a string.

  Workaround: Use MICA modems instead of NextPort modems.

Alternate Workaround: Use ISDN PRI T1 instead of T1 CAS signaling.

- CSCin97717

  Symptoms: Binding interfaces is not happening properly, and A router crashes when trying to bring up user on that interface.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG.

  Workaround: There is no workaround.

- CSCsa63173

  Symptoms: CEF may not be updated with a new path label that is received from the BGP peer.

  If a router configured for BGP IPv4+labels multipath receives a BGP update that only changes the MPLS label for a non-bestpath multipath, the router fails to update the forwarding plane. This results in dropping or mis-branding the traffic.

  Conditions: In a IPv4+labels multipath setup, if a label is changed for the non-bestpath multipath and that is the only change in the new update received from the neighbor, the new label will not be programmed in forwarding, hence there will be label inconsistency between the BGP and the forwarding tables.

  Workaround: There is no workaround.

- CSCsb25337

  Cisco devices running Cisco IOS which support voice and are not configured for Session Initiated Protocol (SIP) are vulnerable to a crash under yet to be determined conditions, but isolated to traffic destined to User Datagram Protocol (UDP) 5060. SIP is enabled by default on all Advanced images which support voice and do not contain the fix for CSCsb25337. Devices which are properly configured for SIP processing are not vulnerable to this issue. Workarounds exist to mitigate the effects of this problem. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsb52900

  Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

  Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

  – The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
  – The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

  This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

  Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsb69271

  Symptoms: The voice path confirmation fails due to time-out while waiting for the DTMF tone.

  Conditions: The channels on the CallGen are timed-out waiting for DTMF tones, sent by the other channels. This is not specific to a particular DTMF tone, this is random.

  Workaround: There is no workaround.

- CSCsb76671

  Symptoms: Intermittent one-way audio (PSTN hears dead air) on inbound ISDN call through Cisco VoIP AS5850 gateway.

  Conditions: This symptom has been observed to occur with inbound ISDN calls with outbound SIP calls towards a Cisco MeetingPlace server. Numerous calls which are transferred via SIP REFER contribute to the gateway get into this state.

  Workaround: There is no workaround to prevent the gateway from getting into this state. Once in this state, reloading the gateway will help clear this condition for awhile.

- CSCsb79608

  Symptoms: The router may crash with DSP-related Decodes as PRI groups are added to the configuration.

  Conditions: This symptom has been observed on a Cisco AS5850 running Cisco IOS Release 12.4(3) in Split Mode. This symptom may occur on other Cisco AS5x00 series routers that utilize the same DSP module.

  Workaround: There is no workaround.

- CSCsb91678

  Symptoms: A software-forced crash may occur on a Cisco 7206VXR because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco 7206VXR that has a low-speed Mueslix-based serial port adapter such as a PA-4T+, PA-8T-V35, PA-8T-X21, or PA-8T-232 port adapter and that runs a Cisco IOS image that integrates the fix for caveat CSCec63468.

  The symptom occurs only for low-speed port adapters such as the PA-4T+, PA-8T-V35, PA-8T-X21, and PA-8T-232 port adapters. The symptom may also affect port adapters in adjacent slots, and not only the port adapters in physically adjacent slots, but also the port adapters that are logically adjacent in the initialization path. This memory corruption occurs in the PCI/IO memory space.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec63468. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround. Note that high-speed or unchannelized serial port adapters are not affected.

  Further Problem Description: The following error messages and tracebacks are generated just before the crash occurs:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
-Traceback= 6074F79C 601BB3AC 601BC72C

%MUESLIX-1-HALT: Mx serial: Serial2/0 TPU halted: cause 0x3 status 0x0043404F
shadow 0x630FB864

%ALIGN-3-SPURIOUS: Spurious memory access made at 0x6074F388 reading 0x1F
%ALIGN-3-TRACE: -Traceback= 6074F388 601BB3AC 601BC72C 00000000 00000000
00000000 00000000 00000000
%ALIGN-3-TRACE: -Traceback= 6074F7C0 601BB3AC 601BC72C 00000000 00000000
00000000 00000000 00000000

%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process
```

```
= Per-Second Jobs.
-Traceback= 607E0078 607E44AC 607DACD0 601B0CD4 601B1A04 601ADEA8 603E2C2C
607CF128 6076E2EC
```

- CSCsc03569

  Symptoms: Incoming and outgoing PSTN calls fail on a BRI interface.

  Conditions: This symptom has been observed on a Cisco 2620XM VoIP Gateway (MGCP) with Cisco IOS Release 12.4(2)T1 and a BRI Backhauled MGCP Gateway controlled by Cisco CallManager release 4.1(3)SR1.

  Workaround: There is no workaround.

- CSCsc11833

  Symptoms: An analog or digital CAS port gets into a state where inbound and/or outbound calls through the port may no longer work.

  Conditions: This symptom has been seen on 2800/3800 gateways with analog or digital CAS ports which use PVDM2 DSP modules.

  It can take some time for the symptom to occur, but when it does occur, it impacts multiple ports which share the same signaling DSP. To see which DSP a port is using for signaling, check the output of the exec command **show voice dsp signa ling**. It has been observed to occur more often with those ports which use DSP 1 on the PVDM2 module for signaling.

  If a problem is noticed only on a single voice port, it would not be this issue.

  Since PRI/BRI does not utilize the DSP for signaling purposes, it is not impacted by this issue.

  When the problem occurs and this is either on a VIC2-xFXO or EVM DID/FXS modulem, run 'test voice port <port #> si-reg-read 39 1' on one of the impacted ports. You need to run "terminal monitor" first to see the output. The output typically should be a single octet value for register 39. When the problem happens, information for Registers 40, 41 and 42 is presented as well and some of the registers show double-octet information. See example output below.

  If using FXS or analog E&M modules, use "test voice port <port #> codec-debug 10 1" and compare the output. Again, the normal output will be single octet information for each register.

  This test only needs to be run on one of the voice ports in this state to confirm if this is the issue being seen.

  Workaround: There is no workaround to prevent this problem from occurring. Once in this state, a reload of the gateway is necessary to recover it.

  Additional Information: If the problem being seen has been confirmed to be this issue, the software changes associated with this report will mitigate the problem in the majority of cases. It may still be possible to see the problem in some cases and if this is experienced contact the TAC for assistance.

- CSCsc12098

  Symptoms: The fix for busyout *slot* on the Cisco AS5400 platform causes build issues.

  Conditions: This symptom is observed on a Cisco AS5400 platform.

  Workaround: There is no workaround.

- CSCsc15366

  Symptoms: If a Media Gateway Control Protocol (MGCP) Create Connection (CRCX) request is received containing a request for a clear-channel codec, the Cisco 1760 router fails to find a matching codec, and the call fails.

  Conditions: This symptom has been observed on a Cisco 1760 router.

Workaround: There is no workaround.

- CSCsc20149

  Symptoms: When you enter the **show voice call status** command five to six times in quick succession, the CPU use of a Cisco AS5850 reaches 99 percent. The Cisco AS5850 thereafter becomes very unstable in accepting incoming calls. This situation can be highly service-impacting under stress conditions.

  Conditions: This symptom is observed on a Cisco AS5850 that is running a special image of Cisco IOS Release 12.3(11)T6 and occurs only when there are more than 900 H.323 voice calls.

  Workaround: Do not enter the **show voice call status** command in a stress situation.

- CSCsc27337

  Symptoms: A Cisco router may reload with a bus error.

  Conditions: This symptom has been observed when IPS is enabled with the MSN Messenger Client DNS Request signature or Yahoo Messenger Client DNS Request signature.

  Workaround: Delete the MSN Messenger Client DNS Request or Yahoo Messenger Client DNS Request signature with the **ip ips signature** *sig-id* **delete** command.

- CSCsc31082

  Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

  The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in **show frame-relay pvc** show the packets correctly.

  Conditions: A map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

  Workaround: There is no workaround.

- CSCsc35321

  Symptoms: A system crash occurs with traceback with mgd_timer_xxx under certain scenarios.

  Conditions: This symptom is observed on a Cisco 3845 router while unconfiguring MGCP after running a CRCX test.

  Workaround: There is no workaround.

- CSCsc39557

  Symptoms: Spurious memory access errors are encountered that may cause a bus error crash.

  Conditions: This symptom is observed on a Cisco 2800 router that is utilizing voice and is running Cisco IOS Release 12.4(3). This appears to be seen only when caller-id is enabled on FXS ports.

  Workaround: Disable caller-id on any FXS ports.

- CSCsc40236

  Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

  Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

  Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc40912

  Symptoms: SNA Switch (SNASw) routers experience a software-forced crash. The following message is seen in the log:

```
validblock_diagnose, code = 1
```

Conditions: This symptom has been observed after issuing an **inact giveback** command at VTAM directed at the router:

V NET,INACT,ID=dlurname,GIVEBACK,FINAL=YES

where *dlurname* is the router CP name.

This symptom occurs during VTAM VARY INACT GIVEBACK processing. This is a regression problem caused by CSCsb11554 so it is only applicable if running Cisco IOS after Cisco IOS interim Release 12.3(15.8), Release 12.4(2.11) and Release 12.4(2.11)T.

Workaround: There is no workaround.

- CSCsc40952

  Symptoms: Phones that are configured for Cisco VT Advantage feature will not register with SRST if they are engaged in SRST fallback operation.

  Conditions: This symptom is observed when using the following:

  - Cisco CallManager Version 5.0 (1.51.225)
  - Cisco 2600 product line for SRST
  - Cisco IOS Release 12.4

  Workaround: Unplug connection to Cisco VT Advantage.

- CSCsc42938

  Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured globally or on an interface.

  Conditions: This symptom is observed when you enter the **show mpls ldp neighbor** command while LDP sessions are coming up or going down.

  Workaround: There is no workaround.

- CSCsc44206

  Symptoms: A Cisco AS5400HPX that is running voice calls with Cisco IOS Release 12.4(3a) has higher CPU utilization than when running Cisco IOS Release 12.3(7) T based images.

  Conditions: This behavior is for all types of voice call configurations.

  Workaround: There is not workaround.

- CSCsc51183

  Symptoms: A Cisco AS5850 may restart because of a software forced crash preceded by the following error:

  ```
  %SYS-6-STACKLOW: Stack for process VTSP running low, 0/12000
  ```

  Conditions: This symptom has been observed on Cisco IOS Release 12.3(11)T.

  Workaround: There is no workaround.

- CSCsc54584

  Symptoms: A standard ingress ACL for transit traffic does not function on an interface that is configured for MFR.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(11)T8 and that has an MFR bundle that is configured on a PA-MC-8TE1 port adapter. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsc68262

  Symptoms: A Cisco 2821 router may crash intermittently if the router switches Encapsulating Security Payload (ESP) packets.

  Conditions: This symptom has been observed on a Cisco 2821 router when switching ESP packets.

  Workaround: There is no workaround.

- CSCsc74783

  Symptoms: Intrusion Prevention System (IPS) signatures that require inspection of TCP flows below port 550 may not be triggered on a Cisco IOS IPS device.

  Conditions: This symptom is observed on a Cisco IOS router that is configured for IPS functionality.

  Workarounds: Apply CBAC (Context Based Access Control) in addition to IPS.

  Further Information: On a Cisco IOS router with IPS (Intrusion Prevention System) enabled, all TCP flows should be subject to TCP stateful inspection until the TCP 3-way handshake is complete. This does not work for TCP sessions with a destination port that is less than 550, if it does not match a predefined signature on the router.

- CSCsc80670

  Symptoms: The on-board FastEthernet 0/0 results in state “FastEthernet0/0 is up, line protocol is down” after a reload, power-up or a shutdown and no shutdown operation. This is verified when the FastEthernet 0/0 is connected to media converters in series.

  This symptom is not present if the Cisco 1718 and Cisco 2950 routers are connected directly, without any media converters in between. This symptom may not be present using a media converter from other vendors.

  Conditions: This symptom has been observed connecting the on-board port of a Cisco 17xx router running Cisco IOS Release 12.3(11)T to media converters in series.

  1718(fa0/0)--media converter----------media converter--(fa 0/1)2950

  This symptom has also been observed with Cisco IOS Release 12.4(5), which is the latest available image for this platform.

  Workaround: Replace the media converter with one from another vendor.

- CSCsc81637

  Symptoms: A Cisco IOS VoIP gateway may reload unexpectedly.

  Conditions: This symptom is observed on a gateway such as a Cisco 2800 series or Cisco 3800 series that supports time-division multiplexing (TDM) hairpinning between voice modules. Under rare circumstances, the gateway may unexpectedly reload when a call is hairpinned between ports on the gateway.

  Workaround: There is no workaround.

- CSCsc94359

  Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

  Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf** *vrf-name network* command on the PE router that has mismatched labels.

- CSCsd11646

  Symptoms: On a router that runs Multiprotocol Label Switching (MPLS), the "%SYS-3-OVERRUN:" and "%SYS-6-BLKINFO" error messages may be generated and a software-forced crash may occur on the router.

  Conditions: This symptom is observed when you enter the **show mpls ldp discovery** command under the following condition:

  - There are multiple LDP adjacencies configured through one interface.
  - The adjacencies between peers through this interface have not been fully established for some peers.
  - The unestablished LDP adjacencies are coming while you enter the **show mpls ldp discovery** command.

  Workaround: Do not enter the **show mpls ldp discovery** command while multiple LDP adjacencies are coming up. Rather, enter the **show mpls ldp neighbor [detail]** command while multiple LDP adjacencies are coming up.

- CSCsd14445

  Symptoms: A router crashes when you unconfigure the resource pool of a customer profile.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.4(5b) or Release 12.4(7) and could also occur in Release 12.4T. The symptom may be platform-independent.

  Workaround: Do not unconfigure a customer profile when an active session on the platform uses the customer profile.

- CSCsd16977

  Symptoms: A crash can be observed by segmentation violation (SegV) on a Cisco 2651XM-V-CCME.

  Conditions: This symptom is observed occasionally when a fax is being sent through the router. This problem has been seen with Cisco IOS Releases 12.3(14) T and later versions through Cisco IOS Release 12.4(5).

  Workaround: There is no workaround.

- CSCsd29364

  Symptoms: Service Selection Gateway (SSG) does not send attribute NAS-PORT [5] on the access request packet for a prepaid service reauthorization.

  Conditions: This symptom occurs when SSG is configured, and User is a prepaid user.

  Workaround: There is no workaround.

- CSCsd30244

  Symptoms: The router crashes on busyout of a CT3 card.

  Conditions: This symptom has been observed only after the router is booted with no T1 configuration on the T3 controller.

  Workaround: There is no workaround.

- CSCsd39519

  Symptoms: A Media Gateway Control Protocol (MGCP) gateway hangs when voice calls come in from either the IP or the PSTN side in which a leg of the call is on a BRI Voice Interface Card (VIC). The gateway stops responding and does not process any traffic. The only way to bring the router back is to power-cycle it.

Conditions: This symptom is observed for every call over a BRI VIC/WIC if the MGCP gateway runs Cisco IOS Release 12.4(4)T1 or later releases. The symptom may also occur in Release 12.4.

Workaround: There is no workaround. The symptom is not observed when the MGCP gateway runs Cisco IOS Release 12.4(4)T.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd46403

  Symptoms: Call comes into an E1 R2 line on a Cisco AS5350 or Cisco AS5400 and gets sent via H323 to an endpoint. The endpoint connects the call, but the Cisco AS5350 or Cisco AS5400 fails to TX ANSWERED on CAS leg resulting in a dead air call.

  Conditions: This symptom occurs on a Cisco AS5350 and a Cisco AS5400 that are running later releases than Cisco IOS Release 12.3(11)T9. Earlier releases are not affected. This symptom also occurs on a Cisco AS5350XM and a Cisco AS5400XM.

  Workaround: There is no a workaround.

- CSCsd58220

  Symptoms: The callee’s phone rings continuously even after the caller goes on- hook.

  Conditions: When the caller goes on-hook, the gateway receives idle and does not recognize the idle. The call does not get disconnected and the callee keeps hearing the ringing tone continuously.

  Workaround: The callee has to pick up the phone for the call to be dropped.

- CSCsd58381

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd67958

  Symptoms: A router acting as Home Agent (HA) may crash when PIM is configured on it. The behavior is seen when a neighbor with a higher Layer3 address tries to become the Designated Router (DR).

  Conditions: The interfaces on HA and its neighbor are configured with sparse- dense mode (PIM). This symptom is observed on a Cisco router that is running Cisco IOS Interim Release 12.4(7.15).

Workaround: If PIM needs to be configured on tunnel interfaces, this crash can be avoided by choosing higher values of tunnel interface number, like "interface tunnel xxxx," which might not have been created by Mobile IP for Mobile IP flows and deleted. Or, PIM needs to be configured on tunnel interfaces before Mobile IP creates any Mobile IP tunnels.

Wide-Area Networking

- CSCed51827

  Symptoms: When you ping a router, the following error message is generated on the router:

  ```
  %IPFAST-2-PAKSTICK: Corrupted pak header for Virtual-Access3, flags 0x80
  ```

  Conditions: This symptom is observed when PPP Multilink (MLP) over L2TP is configured.

  Workaround: There is no workaround.

- CSCed52110

  Symptoms: IP header compression does not function for FR PVC-Bundles.

  Conditions: This symptom is observed when IP header compression is configured for Frame Relay PVC bundles.

  Workaround: There is no workaround.

- CSCeg77994

  Symptoms: A LAC does not send an Accounting-Start RADIUS record to a RADIUS server for a user session.

  Conditions: This symptom is observed on a Cisco platform that functions as a LAC and that runs Cisco IOS Release 12.3(14)T1 when a switchover occurs from one LNS to another LNS while the user session is brought up.

  Workaround: There is no workaround.

- CSCek28575

  Symptoms: A router reloads at the "process_modem_command" function during a test that involves asynchronous media.

  Conditions: This symptom is observed on a Cisco AS5400 but is not platform-dependent.

  Workaround: There is no workaround.

- CSCsc17673

  Symptoms: Using the **show caller full** or **show caller interface Virtual-Access XX full** commands on a PPPoE client interface causes the router to unexpectedly reload.

  Conditions: This symptom has been observed on routers using Cisco IOS Release 12.4(3.3) and later versions.

  Workaround: Avoid using those commands.

- CSCsc30497

  Symptoms: NAS-Port Pre-Auth failure breaks PPPoE session limit per VLAN. Once the authorization fails, local limit does not get applied to a particular interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.3YM.

  Workaround: There is no workaround.

- CSCsc49637

  Symptoms: If a PPPoE client session is timed out (e.g. due to a network outage), and a restart of the session is subsequently unsuccessful (e.g. because network outage persists or the PPPoE server has not timed out the prior session) and if the user then manually clears the session, then the router will no longer be able to bring up this session until a reload is performed.

  Conditions: This symptom has been observed when the PPPoE session is unexpectedly interrupted with Cisco IOS Release 12.3(8)T8 or Release 12.3(11) T5. The next feature also needs to be configured.

  pppoe-client dial-pool-number 1 dial-on-demand

  Workaround: Use the following procedure:

  1. Reload.
  2. Do not configure the DDR feature for the PPPoE session. This problem is limited to PPPoE client sessions using the DDR feature.

- CSCsc66612

  Symptoms: A Cisco router configured for Virtual Private Dialup Network (VPDN) may unexpectedly reload with Bus Error.

  Conditions: This symptom was observed on a Cisco7200VXR series router equipped with NPE-G1 processor card running Cisco IOS Release 12.3(14)T3.

  Workaround: There is no workaround.

  Further Problem Description: The crash was preceded by “SYS-2-INPUT_GETBUF: Bad getbuffer” error messages.

Resolved Caveats—Cisco IOS Release 12.4(5a)

Cisco IOS Release 12.4(5a) is a rebuild release for Cisco IOS Release 12.4(5). The caveats in this section are resolved in Cisco IOS Release 12.4(5a) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCej42445

  Symptoms: MS-CHAP authentication fails with Cisco IOS Release 12.4(5) and MS- CHAP and PAP authentication fails with the Cisco IOS Release 12.4(5)fc2 image

  Conditions: This symptom has been observed when running Cisco IOS Release 12.4 (5) and Release 12.4(5)fc2 while using Tacacs+ with MS chap for authentication.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCsc30369

  Symptoms: A cBus Complex Restart may occur on a Cisco 7500 series when you leave the interface configuration mode after you have changed the encapsulation on a serial interface from HDLC to another encapsulation type such as PPP or Frame Relay. In addition, for interfaces with an MTU of 1500, the maximum datagram becomes fixed to 1608 for interfaces of low-speed serial port adapters and to 1610 for interfaces of high-speed serial port adapters.

  Conditions: This symptom is observed after the first change to the type of encapsulation from the default of HDLC to another encapsulation type when you leave the interface configuration mode. Subsequent changes to the type of encapsulation do not cause the cBus Complex Restart. The overhead added to the MTU is always 24. This will be changed to 108.

  Workaround: There is no workaround for the cBus Complex Restart. You can reconfigure the MTU to prevent packets drop as giants.

  Further Problem Description: When the router boots with the encapsulation type set to the default of HDLC on a serial interface, the maximum datagram size that can be accepted by the interface is set to 1608. When the encapsulation type is changed, the maximum datagram size may change, which causes an internal MTU change. An MTU change on a Cisco 7500 series results in a cBus Complex Restart, which usually means a 15-second to 45-second outage on the router.

IP Routing Protocols

- CSCei93982

  Symptoms: A router that is running Cisco IOS may crash unexpectedly.

  Conditions: NAT must be enabled for this symptom to occur. The problem is seen when an application uses two well known ports: one for source and the other for destination. The outgoing translation is created, but on the return trip, using the previous source port as the destination, NAT may use the incorrect algorithm.

  For example, if a PPTP session is initiated to the well known port 1723 from source port 21 (FTP), then the outgoing packet will create a FTP translation (we look at source information when going from in->out). When the packet is returned, we again look at the source information to know what kind of packet this is. In this case we have the source port will be 1723, and NAT will assume this is a PPTP packet. This will try to perform PPTP NAT operations on a data structure that NAT built for a FTP packet and may lead to a crash.

  Workaround: There is no workaround.

- CSCsb09709

  Symptoms: A router crashes because of a watchdog timeout when you remove a BGP configuration with an IPv6 Address Family Identifier (AFI).

  Conditions: This symptom is observed when you enter the **no router bgp** command for a BGP configuration with an IPv6 AFI.

  Workaround: There is no workaround.

- CSCsb09852

  Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsc41694

  Symptoms: Router hangs while unconfiguring the BGP **no router bgp** command.

  Conditions: This symptom has been observed in Cisco AS5400 and Cisco AS5850 routers having the image c5400-js-mz.123-16.15

  Workaround: There is no workaround.

Miscellaneous

- CSCec16597

  Symptoms: Cisco CallManager controlled MGCP gateways configuration download function always configures "mgcp fax t38 inhibit". If this is changed manually in the Cisco IOS CLI, the configuration download facility will change it back to "mgcp fax t38 inhibit".

  This DDTS removes the code that automatically configures this line.

  If customers are using CCM MGCP fax relay between gateways that are running older Cisco IOS versions, and the Cisco IOS Release 12.4T with this change, the fax connections originating from the gateways that are running previous Cisco IOS versions and terminating on the Cisco IOS Release 12.4T gateway will fail unless "mgcp fax t38 inhibit" is configured on the Cisco IOS Release 12.4T gateway.

  If all gateways in the customer network are running the new Cisco IOS Release 12.4T with this fix, then they may configure which ever mode as desired.

  With the fix to CSCec16597, the configuration utility will neither add nor remove this CLI statement.

  Conditions: There are no conditions.

  Workaround: Use the following command to enable and disable Cisco fax relay:

  [no] ccm-manager fax protocol cisco

- CSCei62522

  Symptoms: ISAKMP SA negotiation is not successful in aggressive mode.

  Condition: This symptom has been observed when testing Radius Tunnel Attribute with HUB and Spoke Scenario using Cisco IOS interim Release 12.4(3.3).

  Workaround: There is no workaround.

- CSCei82163

  Symptoms: A Cisco AS5400 might not release all voice resources for an MGCP call after it is disconnected.

Conditions: This symptom is observed on both the Cisco AS5400 and Cisco AS5850 platforms but is not platform dependent. The symptom is associated with the simultaneous disconnection of a large number of calls.

Workaround: There is no workaround.

- CSCej22786

  Symptoms: A Cisco AS5850 universal gateway reloads unexpectedly with a traceback while voice calls and fax calls are brought up simultaneously.

  Conditions: This symptom has been observed when bringing up more than 500 SIP and H.323 voice calls and 92 T.38 Fax Relay calls.

  Workaround: Bring up voice calls only; do not bring up fax calls.

- CSCej20505

  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

- CSCej42804

  Symptoms: A Cisco Gateway that is running Session Initiation Protocol (SIP) calls might run out of processor memory due to hung SIP calls.

  Conditions: Active and hung calls can be seen using the **show sip-ua calls** command. The following specific scenario will result in a hung call:

  1. The gateway initiates an INVITE.
  2. The gateway receives a 100/180 response.
  3. The gateway sends a CANCEL.
  4. The gateway receives the 200ok for the CANCEL.
  5. The gateway receives an invalid final response for the INVITE (or no final response) and drops the message.

  Each hung call will use a little more memory, and eventually the gateway will run out of memory.

  Workaround: Downgrade to Cisco IOS Release 12.3(14)T3, Release 12.3(11)T6, Release 12.4(2)T1, or Release 12.4(1a).

- CSCej43787

  Symptoms: Issuing a **no mgcp** command reloads the network access server (NAS) unexpectedly. The MGCP gateway crashes and reloads due to Hairpin calls.

  Conditions: The unexpected reload is seen while issuing **no mgcp** command after stress testing. This symptom has been observed on a Cisco AS5850 platform running Cisco IOS Release 12.4(5) and only in an MGCP environment when Hairpin calls are involved.

  Workaround: There is no workaround.

- CSCej50928

  Symptoms: Media Gateway Control Protocol (MGCP) calls fail to land in timeslots 16-31 on E1 controllers.

  Conditions: This symptom is observed in a Cisco AS5850 platform that is running a Cisco IOS Release 12.4(5) image. This symptom is not observed if OGW is a Cisco AS5400 platform. This was not observed in a Cisco IOS Release 12.4 (3.8) image. This may be service impacting as only half of the timeslots can be used for generating calls.

  Workaround: There is no workaround.

- CSCej53240

  Symptoms: The system can run out of memory with voice calls over a period of time. With the system handling a large number of voice calls (greater than 50), running the **show memory summary** command periodically will indicate memory in use is increasing.

  Under these conditions, the **show memory debug leak chunks** command shows that there is a memory leak.

  A sample output of this command when the problem is seen is shown below: Chunk Elements:

  ```
  Address  Size  Parent   Name
  45ACC8C8  2052 45786824 (VTSP EVENT poo)
  45ACD0D0  2052 45786824 (VTSP EVENT poo)
  45ACD8D8  2052 45786824 (VTSP EVENT poo)
  ```

  Conditions: This issue is likely to be seen when the system is handling a large number of voice calls (greater than 50). This issue is present in Cisco IOS Release 12.4(5).

  Workaround: Reload the system to recover from this condition.

- CSCek01162

  Symptoms: When removing the OSPF IPsec authentication configuration from CLI in IPV6, an alignment traceback will be seen pointing back to crypto_ikmp_peer_is_dead.

  Conditions: This symptom occurs when OSPF IPsec authentication (IPV6) is configured and removed.

  Workaround: There is no workaround.

- CSCin97574

  Symptoms: Service Selection Gateway (SSG) sends invalid Radius Access Reject packet to a network access server (NAS).

  Conditions: This symptom is seen with SSG in radius proxy mode when AAA server is unreachable.

  Workaround: There is no workaround.

- CSCin97815

  Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in the **show frame-relay pvc** command show the packets correctly.

Conditions: A map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

Workaround: There is no workaround.

- CSCsb54961

  Symptoms: A Cisco gateway may fail to initiate a T.38 call to a third party gateway. When the third party gateway sends T.38 open logical channel to the Cisco gateway, no open logical channel acknowledgement is sent by the Cisco gateway. After waiting for 30 seconds for T.38 open logical channel acknowledgement, the third party gateway closes its T.38 open logical channel.

  Conditions: This happens when T.38 fax relay calls are originated or terminated on a Cisco gateway that is running Cisco IOS Release 12.3(4)T and later releases.

  Workaround: There is no workaround.

- CSCsb58313

  Symptoms: After running a few days, assertion failed at WA_NP_QWRITE and then crashed.

  Conditions: This symptom occurs when running the **show diag** command at high CPU.

  Workaround: Do not run the **show diag** command.

- CSCsb67539

  Symptoms: A Voice Gateway crashes when running under a heavy voice call load.

  Conditions: This symptom is observed on a Voice Gateway that is running Cisco IOS Release 12.3(11)T6. The gateway is under heavy voice call load with access to media/application documents residing on local gateway flash, http and tftp servers.

  Workaround: The following is not quite a workaround:

  call threshold global *cpu-5sec* **low** *value* **high** *value*

  For example:

  call threshold global *cpu-5sec* **low** *50* **high** *70*

  The CLI can ease the CPU load on the gateway by reducing the probability for a crash.

- CSCsb77885

  Symptoms: IKE negotiation will fail. Any tunnel that requires IKE to successfully negotiate a security association will not work.

  Conditions: This symptom occurs when authentication for IKE is configured as RSA encryption (authentication rsa-encr).

  Workaround: There is no workaround.

- CSCsb85136

  Symptoms: When running TCL/VxML applications that perform Media Playing, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: Cisco IOS Media Play code was forgetting to release a memory at the end of media play.

  Workaround: Upgrade to Cisco IOS Release IOS 12.4(3b) if available. If not, contact Multiservices TAC (IOS) and request a patch.

- CSCsb91807

  Symptom: The memory utilization increases.

  Conditions: This symptom has been observed when SSG along with a service profile attribute of "attribute 26 9 251 "Z" " is configured.

  Workaround: There is no workaround.

- CSCsb97185

  Symptoms: A router configured with a 36-port EtherSwitch Module may reload due to memory corruption in the I/O memory pool.

  Conditions: The router must have a 36-port ESW module.

  Workaround: Disable the **ip igmp snooping** command.

```
Router(config)#no ip igmp snooping
Router#show ip igmp snooping
vlan 1
----------
  IGMP snooping is globally disabled
  IGMP snooping is disabled on this Vlan
  IGMP snooping immediate-leave is disabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

- CSCsc00587

  Symptoms: PRI backhauled to MGCP cannot fallback into h323 mode for SRST as there is a hung call. It can be seen in the **show call active voice brief** command but if there is no calls there, definitely check the**show voice vtsp call** command. There will be a call in "S_WAIT_RELEASE" state and cannot be cleared even though ISDN status shows no active calls on that PRI.

  Conditions: This symptom is normally seen when connection from a gateway to CCM flaps. If a call hits the gateway during a transition (fallback switchover or vice versa), the call gets stuck and causes all other PRIs to clock up. The PRI is able to be backhauled to CCM with a hung call but it is not able to fallback into SRST (gateway terminated). With just one call hung, all other backhauled PRIs are affected and cannot fallback in h323. Calls inbound get a "fast busy--- isdn setup" message and is ignored by the gateway as it thinks PRI is still backhauled, so the PRIs are in limbo.

  Workaround: Reload the router.

- CSCsc09246

  Symptoms: The following commands used for detecting memory leaks would crash the router which uses external memory such as the RPM-XF platforms.

  show memory debug leaks show memory debug leaks chunks show memory debug leaks largest show memory debug leaks summary

  Conditions: This symptom has been observed on the RPM-XF cards using Cisco IOS interim Release 12.4(4.6).

  Workaround: There is no workaround.

- CSCsc12570

  Symptoms: The codec upspeed (i.e., G729 to G711ulaw) or downspeed (i.e., G711ulaw to G729) does not happen. Other packet stream-related call parameter changes, such as VAD and PLAYOUT, do not happen as expected.

  Conditions: This symptom has been observed when the codec type or other packet stream parameters are modified using MDCX or through the TDM side of the call module like VTSP.

Workaround: There is no workaround.

- CSCsc13844

  Symptoms: After loading "flash:c2600-entservicesk9-mz.123-11.T7.bin", the E1 controller is missing from the **snmpwalk** command of IF-MIB.

  Conditions: This symptom has been observed on a Cisco2621XM.

  Workaround: There is no workaround.

- CSCsc14106

  Symptoms: If the called party answers a call in the middle of a prompt, one-way voice occurs.

  Conditions: This symptom has been observed when a TCL application tried to play a prompt while a call is alerting and the call is answered before the prompt play is complete. If the call is answered after the prompt play is done, the symptom is not seen.

  Workaround: In the script, connection destroy and reconnect are handled to make sure a reconnect happens. This symptom is now fixed in Cisco IOS.

- CSCsc21674

  Symptoms: PSTN is sending in an "*" and the router is reading it in as a ìDî. PSTN is also sending in a "#" and router is reading it in as an "*".

  Conditions: This symptom has been observed on an MGCP T1-CAS gateway connected to Cisco CallManager doing MF and using Cisco IOS Release 12.3.8.T11, Release 12.3.11.T7, or Release 12.3.14.T4..

  Workaround: There is no workaround.

- CSCsc41913

  Symptoms: A Cisco IOS gateway using Cisco IOS Release 12.3(8)T or later versions will use an ephemeral port to send a response to any SIP request. This may not work with port restricted NAT, which is expecting a response on the same connection as the one on which the request was sent and may drop the response.

  Conditions: This symptom is observed on a Cisco IOS gateway with Cisco IOS Release 12.3(8)T or later releases and a port restricted NAT.

  Workaround: There is no workaround.

- CSCsc44237

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: A switch or router that is either configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

  The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

  Condition 1: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

  Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

  Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

Condition 2: This symptom observed on a Cisco 2811 and Cisco 3845 and occurs only in Cisco IOS Release 12.2(30)S, interim Release 12.4(2.10), and interim Release 12.4(2.10)T, or in any later releases.

Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf** *vrf-name* command is configured, enter the **ip vrf forwarding** *vrf-name* command on at least one interface that has PIM enabled.

- CSCsc64530

  Symptoms: A Cisco 3745 router does not boot up when booting a Cisco IOS with the fix of CSCec74317.

  Conditions: The nvram in the router should be in corrupted state.

  Workaround: Turn the router off and then back on one time will resolve the issue.

- CSCsc64985

  Symptoms: Whenever a voice call is completed, some errant informational messages are echoed to the console and any open Telnet sessions, even though no debugs are enabled. For example, for a DSPless POTS-to-POTS hairpin call, we might see:

```
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  PAK_SUPRESS
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  NSE_PAYLOAD
Nov 30 00:10:37.809 EST:                  SEQ_NUM_START
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  NSE_PAYLOAD
Nov 30 00:10:37.809 EST:                  SEQ_NUM_START
```

  Conditions: This behavior is observed on any Cisco IOS voice gateway which is running a Cisco IOS version listed or implied by the "First Fixed-in Version" field of bug ID CSCsc12570 "mgcp does not switch codec (e.g. g711 to g729) during call".

  Workaround: Use a build of Cisco IOS earlier than those listed or implied by the "First Fixed-in Version" field of bug ID CSCsc12570 "mgcp does not switch codec (e.g. g711 to g729) during call".

- CSCsc66658

  Symptoms: Ping does not work if loopback is configured on the interface.

  Conditions: This symptom has been observed when loopback is configured.

  Workaround: There is no workaround.

- CSCsc76982

  Symptoms: Configuring an ephone-dn number can cause a crash due to an infinite loop.

  Conditions: This symptom has been observed while configuring a "number" under an **ephone-dn** command on a router running Call Manager Express (CME).

  Workaround: There is no workaround.

Protocol Translation

- CSCei15942

  Symptoms: You may not be able to download a complete file from an FTP during a V.120 session.

  Conditions: This symptom is observed on a Cisco AS5400 and Cisco AS5850 that runs Cisco IOS Release 12.2(15)ZK6 or Release 12.3(11)T5. The symptom could also occur in other releases such as Release 12.3 or Release 12.4.

  Workaround: This problem can be circumvented by disabling the negotiation of multilink on the client adapter or the router. Alternatively, configuring **ppp multilink queue depth fifo 10** on the Virtual-Template interface should allow for a successful FTP download.

TCP/IP Host-Mode Services

- CSCsb51019

  Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state and the following error message is generated:

  ```
  %TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco 12000 series.

  Workaround: There is no workaround.

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

  Further Problem Description: BGP in Cisco IOS Release 12.0S and Release 12.4 is not affected because the retransmit timeout is disabled for BGP in these releases.

Wide-Area Networking

- CSCej73049

  Symptoms: AAA method may fail on calls in the Cisco IOS 12.3(11)T releases.

  Conditions: This symptom was observed on a Cisco AS5850 that was running Cisco IOS Release 12.3(11)T8 but is not platform dependent.

  Workaround: There is no workaround.

- CSCsb89292

  Symptoms: ISDN NFAS failover issues are observed in Cisco IOS Release 12.3(11) T7. If the primary NFAS d-channel is bounced, the switch sees some of the b- channels in "remote busy" (RMB).

  Conditions: This symptom only happens when the primary NFAS d-channel is bounced.

  Workaround: There is no workaround.

- CSCsc59584

  Symptoms: Cisco IOS Release 12.4(3) and Release 12.4(5) GROUP SERVICE messages are not correct to the PGW.

  Conditions: The following actions will result in all circuits on the PGW to remain in MATE_UNAVAIL state.

  – Set the IUA destination to out of service (OOS) and then set it to in-service.
  – Set the IUA association to out of service (OOS) and then set it to in-service.
  – Restart the PGW.

  Workaround: Reload the IUA to clear the circuits.This is unacceptable to a live customer.

Resolved Caveats—Cisco IOS Release 12.4(5)

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(5). All the caveats listed in this section are resolved in Cisco IOS Release 12.4(5). This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- 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.

- CSCeg22972

  Symptoms: The output of the **show processes cpu** command shows that the total CPU use is less than the interrupt CPU use.

  Conditions: This symptom is observed on a Cisco platform that continuously routes unicast IPv6 traffic with 70 bytes per packet and 300,000 packets per second when one particular counter that counts interrupt trailing overflows.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat increases the size of the counter.

- CSCeh82694

  Symptoms: A router crashes when an snmpwalk is performed on the ifTable.

Conditions: This symptom is observed when an interface that is registered for high capacity (HC) counters deregisters directly.

Workaround: Disable SNMP or do not poll the ifTable through SNMP.

- CSCei17254

  Symptoms: A router crashes when an SNMP get operation is performed on the CISCO-NETFLOW-MIB for export statistics.

  Conditions: This symptom is observed on a Cisco 7500 series that has an RSP but is platform-independent.

  Workaround: Do not use the CISCO-NETFLOW-MIB.

- CSCei37916

  Symptoms: A Cisco GGSN does not function properly when wait-accounting and AAA Broadcast Accounting are configured on an APN. When the first RADIUS server responds to an Accounting Start message, the GGSN establishes the PDP context without waiting for responses from all other RADIUS servers. Under a stress condition, the GGSN may reload.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 and GGSN Release 5.2 and occurs only when both wait-accounting and AAA Broadcast Accounting are configured together on an APN.

  Workaround: There is no workaround.

- CSCsb14371

  Symptoms: A Cisco 7500 series may log the following error message even if no VIP is installed in slot 0:

  ```
  %IPC_RSP_CBUS-3-NOHWQ: Hardware queue for card at slot 0 not found
  ```

  Conditions: This symptom is observed after a crash of another VIP has occurred. Sometimes the symptom occurs when a VIP is installed in slot 0 but most of the time there is no VIP in slot 0 when the symptom occurs.

  Workaround: There is no workaround.

- CSCsb27960

  Symptoms: When the local method is used at the beginning of a PPP authentication method list and when a user does not exist in the local database, failover to the next method in the method list does not occur. This situation prevents users that are listed in the database of a RADIUS or TACACS+ server from being authenticated.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA.

  Workaround: Temporarily remove the local method from the beginning of the method list.

- CSCsb47733

  Symptoms: A traceback is generated during an SNMP operation.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsb49500

  Symptoms: SNMP traps do not function, preventing an SNMP notification view from being properly associated with a default group that was created via the **snmp-server host** command.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3T, 12.4, or 12.4T.

Workaround: Enter the **show snmp view** command to obtain the SNMP notification view and then apply this view to the default group that was created via the **snmp-server host** command.

- CSCsb86257

  Symptoms: When a named ACL is used at a vty line on an PE router with an interface that is configured in an VPN VRF, making a Telnet connection from this VRF on the interface that is part of the VRF is accepted even though the **vrf-also** keyword is not configured in the **access-class** *access-list-number* command.

  When a regular numbered ACL is used, an incoming Telnet connection from an interface that is part of a VRF is rejected without the **vrf-also** keyword being configured in the **access-class** *access-list-number* command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an MPLS VPN environment and that has VPN VRFs configured.

  Workaround: Use a numbered ACL instead of a named ACL on vty lines on a PE router.

Interfaces and Bridging

- CSCee22523

  Symptoms: A VIP that contains a PA-A3-OC12 ATM port adapter may unexpectedly reload.

  Conditions: This symptom is observed on a Cisco 7500 series that functions in an ATM LANE configuration.

  Workaround: There is no workaround. The traffic on the VIP is disrupted until the VIP comes back up.

- CSCei25164

  Symptoms: A Cisco 7xxx series router may crash because of a bus error exception and may report CPUHOG message when you perform an OIR of an ATM PA-A3 or ATM PA-A6 port adapter.

  Conditions: This symptom is observed on a Cisco 7xxx series router that runs Cisco IOS Release 12.3 when PVC auto-provisioning is enabled on the ATM PA-A3 or ATM PA-A6 port adapter and when many PPP sessions are in transition.

  Workaround: There is no workaround.

- CSCsa94345

  Symptoms: PVCs in an auto VC range stop passing traffic. The output of the **show atm pvc** command does not show the PVC as existing on the router.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is configured with an NPE-G1 and that runs Cisco IOS Release 12.3(14)T, Release 12.4, or Release 12.4T when the router is configured to aggregate PPPoA DSL users.

  Workaround: There is no workaround.

  Further Problem Description: The following sample configuration illustrates the symptom:

```
interface ATM1/0.10 multipoint
   no ip mroute-cache
   atm pppoa passive
   range pvc 10/50 10/100
       encapsulation aal5mux ppp Virtual-Template1
       create on-demand
```

- CSCsb24062

  Symptoms: When you delete a QinQ subinterface, services on all other QinQ subinterfaces are permanently disrupted. For example, PPPoE sessions on all other QinQ subinterfaces are terminated and cannot be brought up again. An attempt to recreate the deleted QinQ subinterface fails because of the unavailability of the **second-dot1q** keyword in the parser, and spurious memory access tracebacks are generated.

  Conditions: This symptom is observed when there are more than 255 QinQ subinterfaces configured with the same outer dot1q VLAN ID and when some of these subinterfaces are subsequently deleted.

  Workaround: Ensure that there no more than 255 QinQ or single dot1q subinterfaces with the same outer (or only) VLAN ID.

  Alternate Workaround: Do not delete the subinterfaces. Even deconfiguring the **encapsulation dot1q** *vlan-id* command does not provide a solution. Rather, just remove all service attributes from the subinterface by entering the **no pppoe enable** command.

- CSCsb51879

  Symptoms: A Cisco 7500 series may generate the following error message and traceback:

  ```
  %IPC-2-ONINT: Invalid operation at interrupt level: IPC blocking send request 103000C
  -Traceback= 40857C4C 40291754 40291AC4 40295214 4028BD1C 4028BBA0 4026C5A8 4075FF30
  407615F0
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a PA-MC-xT1/E1 type of port adapter.

  Workaround: There is no workaround.

- CSCsb65340

  Symptoms: An interface may not be able to receive OSPF hello packets.

  Conditions: This symptom is observed after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the peer interface, causing a link up/down event to occur.

  Workaround: Reconfigure OSPF.

  Further Problem Description: The symptom occurs because the address filter entry is deleted during the link up/down event. You can verify that the symptom has occurred in the output of the **show controller** command and you can manually confirm the deletion of the OSPF MAC entry. When you reconfigure OSPF, the OSPF MAC entry is re-inserted in the address filter.

- CSCsb84265

  Symptoms: PPP LCP negotiation on a LAC fails for ISDN.

  Conditions: This symptom is observed on a Cisco platform that functions as a LAC and that is configured with PA-MC-8TE+ port adapters.

  Workaround: There is no workaround.

- CSCsc05213

  Symptoms: ISDN L2TP sessions cannot be brought up.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4 or Release 12.4T and that is configured with a PA-MC-8TE1+ port adapter that functions in T1 mode. The symptom is platform-independent and could also occur in Release 12.3.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCec85835

  Symptoms: When RSVP and IP header compression are configured on an interface, the output of the **show ip rsvp installed detail** command shows a compression factor of 0, and some of the flow is treated as non-conformant.

  Conditions: This symptom is observed on a Cisco router that is configured for RSVP and IP header compression on interfaces that are configured for fast-switching or CEF-switching.

  Workaround: Enter the **ip rsvp flow-assist** command on the outbound interface of the flow.

- CSCef19137

  Symptoms: There are duplicate entries in the flow cache after an interface bounces, causing packet loss. The output of the **show ip cache flow** command may show information similar to the following:

```
SrcIf      SrcIPaddress    DstIf    DstIPaddress    Pr SrcP DstP      Pkts
Gi0/0.1    10.2.0.1        Fa2/0    10.3.0.1        06 2C26 00B3      5
Gi0/0      10.2.0.1        Null     10.3.0.1        06 2C26 00B3<<<<  7
```

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that runs Cisco IOS Release 12.2(20)S4 when an interface bounces quickly and when the CEF structures are flushed while the ARP cache is not flushed. This situation causes incomplete adjacencies because the CEF process expects a fresh ARP entry to complete its adjacency. The symptom is platform-independent and may also occur on other platforms when the same conditions occur.

  Workaround: Clear the ARP cache or enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCeg57155

  Symptoms: A ping, Telnet traffic, FTP traffic, and trace route traffic across a VRF-aware NAT do not function.

  Conditions: This symptom is observed on a Cisco router that is configured for VRF-aware NAT only when the router is not directly connected to a gateway.

  Workaround: There is no workaround.

- CSCeh35659

  Symptoms: When the **ip bgp fast-external-fallover permit** interface configuration command is enabled on the main interface of a 4-port Gigabit Ethernet ISE line card and on a subinterface of a connected BGP neighbor, and when you enter the **shutdown** interface configuration command on the main interface, the BGP session that is established on the subinterface remains up for about 150 to 180 seconds before the BGP hold timer causes the session to go down.

  Conditions: This symptom is observed on a Cisco 12000 series in a per-interface fast external fallover configuration on a 4-port Gigabit Ethernet ISE line card. However, the symptom may also occur on other platforms that function in a BGP configuration.

  Workaround: There is no workaround. Note that the **ip bgp fast-external-fallover permit** command is currently not supported on subinterfaces.

- CSCeh53906

  Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths** *number-of-paths* command has a value of three or more.

Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

- CSCeh56158

  Symptoms: The **ip nat outside source static** command does not translate the destination IP address of GRE packets.

  Conditions: This symptom is observed when the source IP address of GRE packets is translated by the **ip nat inside source** command.

  Workaround: Workaround it's to use pool overload translation.

- CSCeh92012

  Symptoms: Border Gateway Protocol (BGP) next-hop information is not redistributed as expected by Open Shortest Path First (OSPF).

  Conditions: This symptom is on a Cisco 7206VXR that is configured with an NPE-G1 (revision A) and that runs Cisco IOS interim Release 12.4(1.8)T. However, the symptom is platform-independent and occurs also in other releases.

  Workaround: There is no workaround.

- CSCei06089

  Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

- CSCei13040

  Symptoms: When an OSPF neighbor comes back up after a very fast (sub-second) interface flap, OSPF routes that are learned via the interface that flapped may not be re-installed in the RIB.

  Conditions: This symptom is observed when the following two events occur:

  – The interface flaps very quickly.

  – The neighbor comes back up before the LSA generation timer expires.

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

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

- CSCei16615

  Symptoms: A neighbor reloads when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an LSP router that functions as a tunnel headend.

  Conditions: This symptom is observed when the following events occur:

  - The tunnel headend sends a Path via RSVP to the neighbor but the Resv message is delayed.

  - There is only one Path to the neighbor for the session.

- At the neighbor, the cleanup timer for the Path expires before the Resv message arrives, causing the session to be terminated.

Workaround: There is no workaround.

- CSCei21133

  Symptoms: A router reloads because of a watchdog timeout when you perform an snmpwalk.

  Conditions: This symptom is observed on a Cisco 7200 series but may be platform-independent. The traceback stack decode points to an EIGRP function although EIGRP is not configured on the router.

  Possible Workaround: Configure a dummy EIGRP router process, for example one for which the network covers only a loopback interface, so that the snmpwalk does not cause the router to crash.

- CSCei26899

  Symptoms: When you reset a BGP peer, some prefixes are missing.

  Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- CSCei27084

  Symptoms: Configured NAT pools are not shown in the startup configuration and are not visible through CLI commands.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when you configure NAT pools after you have first configured a discontiguous NAT pool.

  Workaround: If you need only a single discontiguous NAT pool, configure it after you have configured other NAT pools.

- CSCei36960

  Symptoms: On a router that is configured with a Context-based Access Control (CBAC) firewall, NAT may not work properly, causing routing errors.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.3(14)T when the router has the **ip nat outside static network** *global-network local-network mask* command enabled and when the command points to a serial interface that is configured for both CBAC and NAT.

  Workaround: Use a static route for the *global-network* argument. If this is not an option, there is no workaround.

- CSCei50937

  Symptoms: A router may reload when you the configuration from “classic NAT” to NVI.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4(2)T.

  Workaround: There is no workaround.

- CSCei58597

  Symptoms: When you enter the **show running-config** or **process-min-time** command, a spurious memory access or crash may occur.

  Conditions: This symptom is observed on a Cisco router that is configured for OSPFv3.

  Workaround: There is no workaround.

- CSCei65865

  Symptoms: When an RSVP application (for example, the MPLS TE feature) sends an updated Path message to reflect a modification in its QoS request, the updated Path message may not be forwarded by a downstream RSVP-aware router.

  Conditions: This symptom is observed when the downstream RSVP-aware router has two RSVP features configured: local policy and refresh reduction. The commands to configure these features are the **ip rsvp policy local** command and the **ip rsvp signalling refresh reduction** command, respectively.

  When an RSVP reservation is established with a Path/Resv message handshake and the sender application subsequently transmits an updated Path message that the downstream router applies to an RSVP local policy, the router does not forward the modified Path message. This situation prevents the application from receiving the corresponding Resv message, and may cause the application to fail.

  Workaround: If this is an option, unconfigure the local RSVP policy or refresh the reduction and then restart the RSVP application. If this is not an option, there is no workaround.

- CSCei71446

  Symptoms: A router crashes when the IP address of a GRE tunnel is changed to an unnumbered loopback address.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3).

  Workaround: Remove all **ip unnumbered** commands that point to the original numbered interface before you configure this numbered interface as an unnumbered interface itself.

  Alternate Workaround: Change all unnumbered interfaces to point to the new parent.

- CSCei75375

  Symptoms: OSPFv3 may write zeros into single words of memory in the heap. Depending on what (if anything) is allocated at the address that is being cleared, the router may reload or fail in some other way.

  Conditions: This symptom is observed only when an OSPFv3 process or area is unconfigured or when you enter the **clear ipv6 ospf process** command and when both of the following conditions are present:

  – The area that is removed or the process that is cleared contains one or more non-self-originated type-4 LSAs.

  – The router does not have an intra-area path to an ASBR that is described by the type-4 LSA.

  Workaround: There is no workaround.

- CSCei78815

  Symptoms: The EIGRP MIB subsystem is missing.

  Conditions: These symptoms are observed on a Cisco platform that runs Cisco IOS Release 12.3T or Release 12.4 and may also occur in Release 12.4T.

  Workaround: There is no workaround.

- CSCei83265

  Symptoms: MVPN traffic is limited to about 9 Mpps and the CPU usage on the egress line card is 100 percent.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when MVPN performs decapsulation in the slow path instead of the fast path.

Workaround: There is no workaround.

- CSCei86031

  Symptoms: When the **distribute-list route-map** *map-tag* command is used under the OSPF router mode and when the route map is modified, OSPF does not update the routing table based on the changes in the route map.

  Conditions: This symptom is observed when a route map that is referenced in the **distribute-list route-map** *map-tag* command is modified.

  Workaround: Enter the **clear ip ospf** *process id* command or the **clear ip route *** command.

- 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.

- CSCsa75512

  Symptoms: A crash that is related to OSPF flooding may occur on a Cisco router that is configured for OSPF and MPLS traffic engineering.

  Conditions: This symptom is observed when 1600 OSPF interfaces are configured in an OSPF area that is also configured for MPLS traffic engineering and when OSPF interfaces and OSPF adjacencies flap. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef16096. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Reduce the number of OSPF interfaces in the OSPF area to 300 or less. You can check the number of OSPF interfaces by entering the **show ip ospf** or **show ip ospf interface** *interface-type interface-number* **brief** command. Note that all interfaces that are covered by network statements are counted.

- CSCsb13988

  Symptoms: A router that is configured for NAT may crash because of a bus error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(9a) but is not platform-specific. The crash occurs while NAT attempts to translate an IP address in an H.323 RAS messages that does not contain an IP address.

  Workaround: Disable H.323 RAS in NAT by entering the **no ip nat service ras** command. If you must use H.323 RAS in NAT, there is no workaround.

- CSCsb22290

  Symptoms: On a Cisco router that is configured for Port Address Translation, when you enter the **ip nat service fullrange udp port** *port-number* command, the port-allocation logic does not function. When a PAT port is already taken, the next-port logic fails, causing some packets to be discarded.

  Conditions: This symptom is observed on a Cisco IOS Mobile Wireless Gateway (MWG) that is configured for high availability (HA). However, the symptom may occur on any platform that has the **ip nat service fullrange udp port** *port-number* command enabled.

  Workaround: Disable the **ip nat service fullrange** command.

  Further Problem Description: Regular PAT and NAT are not affected. Only the port-allocation logic in relation to the **ip nat service fullrange** command is affected.

- CSCsb23433

  Symptoms: IP multicast packets are lost until the next periodic PIM (S,G) Join message.

  Conditions: This symptom is observed in the following scenario:

  When there is an intermittent source that is not active for 3.5 minutes, the (S,G) entry expires on the local RP and transit routers, but because the MSDP SA cache expiration timer is 6 minutes, the local RP continues to send MSDP SA messages with a 1 minute interval, which refreshes the (S,G) entry on the remote RP. When the source starts after 3.5 minutes of inactivity, it is registered with the local RP, and an MSDP SA message with an encapsulated packet is sent to the remote RP. However, the remote RP does not sent a PIM (S,G) Join message to the source because the remote RP still has an (S,G) entry present.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdp44494. Cisco IOS software releases that re not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCsb25662

  Symptoms: When an IP phone that is located at a central site leaves a conference, a one-way voice condition occurs for the remaining two phones in the conference.

  Conditions: This symptom is observed in a Hub-and-Spoke configuration in which both sites perform NAT when a voice conference is created by an IP phone that is located at a central site with two IP phones that are located at a remote site. NAT is configured on the hub and at the remote site, SCCP is the voice signaling protocol, and the conference occurs between the hub and the remote site.

  Workaround: Enter the **clear ip nat translation *** command.

- CSCsb32141

  Symptoms: A router that is configured for Resource Reservation Protocol (RSVP) generates the following error messages on the console and then crashes:

  ```
  %LINK-0-REENTER: Fatal reentrancy, level=3, intfc=FastEthernet0/1
  -Process= "RSVP", ipl= 3, pid= 251
  %SYS-6-STACKLOW: Stack for process RSVP running low, 0/24000
  ```

  Conditions: This symptom is observed when the **ip rsvp bandwidth** and **service-policy output** commands are configured on the same interface and when the policy map for the service policy is configured with the **fair-queue** command.

  Workaround: Enter the **ip rsvp resource-provider** *none* command on the interface.

Alternate Workaround: Enter the **ip rsvp bandwidth** *value* command and ensure that the *value* argument is equal to the value that is displayed on the "Available Bandwidth" line in the output of the **show interface** *interface* command plus the value that is shown in the "allocated" column in the output of the **show ip rsvp interface** command.

- CSCsb34946

  Symptoms: When you add a second redundancy group, a router reloads and generates a traceback.

  Conditions: This symptom is observed on a Cisco router that is configured for HSRP and that has Stateful NAT configured and bound to the HSRP group.

  Workaround: There is no workaround.

- CSCsb35522

  Symptoms: Routers that are configured for Stateful NAT do not register each other when they are associated with an HSRP group that is configured on a VRF-aware interface.

  Conditions: This symptom is observed when the following conditions are present:

  – Redundant Cisco routers are connected to LAN segments.
  – The connectivity to the LAN is based on physical interfaces and a trunk.
  – Each interface/subinterface is assigned to a unique VRF.
  – Stateful NAT is configured to share the translation table between the active and standby translators.

  Workaround: Map the IDs of the various VRFs that are associated with the HSRP group. However, this workaround has the limitation that one interface has to be spared on the LAN. This situation could be a constraint if the network is configured in such a way that all interfaces have VRF enabled.

- CSCsb36589

  Symptoms: A router that is configured for OSPFv3 may crash because of memory corruption or a CPUHOG condition.

  Conditions: This symptom is observed rarely in a configuration with a large LSA with at least 44 links that have OSPFv3 enabled and with some links configured for broadcast mode when an adjacency with a peer router flaps.

  Workaround: There is no workaround.

- CSCsb36755

  Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP multipath.

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

- CSCsb37698

  Symptoms: When you configure NAT, an IPv6 configuration is evoked unintentionally in addition to the NAT configuration.

  Conditions: This symptom is observed when you enter the **ip nat pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command. When you do so, the output of the **show running-config** command shows the above-mentioned command and, in addition and unexpectedly, also the **ipv6 nat v6v4 pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command.

  Workaround: There is no workaround.

- CSCsb54823

  Symptoms: One router (R2) may begin sending updates to another router (R1) before R2 has received the BGP prefix list from R1.

  R1 does apply its inbound BGP prefix list so routes are denied if they need to be. However, R2 sends routes to R1 which are denied by R1.

  Conditions: This symptom is observed when both routers have negotiated a BGP outbound route filter (ORF) and when R1 sends its BGP prefix list to R2.

  Workaround: There is no workaround.

- CSCsb61487

  Symptoms: A (*,G) prune is not processed on a non-Designated Router (DR), causing a link that is shut down on a DR router to continue to receive multicast packets.

  Conditions: This symptom is observed in a configuration with a DR router that has a link (link A) to a PIM neighbor and a backup router that has a link (link B) to another PIM neighbor. The symptom occurs when you shut down link A and bring up link B. The OIL of the DR router is Null on (S,G) but on its PIM neighbor, the OIL on (S, G) still points to the interface that is connected to the DR router, that is, to link A. The OIL on the PIM should be pruned immediately, but it takes three minutes before this occurs. This situation causes the DR router to continue to receive multicast packets until the OIL on the PIM is finally pruned.

  Workaround: There is no workaround.

- CSCsb61846

  Symptoms: A Cisco 2811XM that is configured for Stateful Fail-over Network Address Translation (SNAT) may unexpectedly crash because of a bus error.

  Conditions: This symptom is observed when the Cisco 2811XM runs with a heavy traffic load and when SNAT exchanges occur at a high rate when the crash occurs.

  Workaround: There is no workaround.

- CSCsb74588

  Symptoms: A router that is configured for OSPFv3 may crash because of memory corruption or a CPUHOG condition.

  Conditions: This symptom is observed rarely in a configuration with a large LSA with 64 parallel links that have OSPFv3 enabled in broadcast mode when all adjacencies with a peer router flap.

  Workaround: There is no workaround.

- CSCsb79749

  Symptoms: The output of the **show memory summary** command may contain garbled characters in the “What” column.

  Conditions: This symptom is observed when you configure OSPF with at least one network, and then unconfigure it.

  Workaround: There is no workaround.

- CSCsb85290

  Symptoms: Reverse Path Forwarding may not occur for IPv6 packets.

  Conditions: This symptom is observed on a Cisco platform that functions as an IPv6 Bootstrap Router (BSR).

  Workaround: There is no workaround.

ISO CLNS

- CSCei04683

  Symptoms: A router may advertise an IPv6 default route into a level-2 topology.

  Conditions: This symptom is observed when the following conditions are present:

  - The router runs the IS-IS routing protocol on both level 1 and level 2.
  - The router advertises IPv6 prefixes.
  - The router has the IS-IS ATT bit set.
  - The router has level-1 connectivity to another level-1/level-2 IS-IS router.
  - An SSO switchover occurs on the router or the router loses and then regains connectivity to the level-2 topology.

  Workaround: Trigger a change that causes the router to regenerate its level-2 LSP.

- CSCei12603

  Symptoms: A 30 to 40 ms interruption in traffic forwarding may occur when you modify the **tunnel mpls traffic-eng bandwidth** command for an MPLS traffic-engineering tunnel.

  Conditions: This symptom is observed on a router that is configured for MPLS traffic engineering with IS-IS as the associated IGP.

  Workaround: There is no workaround.

- CSCei58655

  Symptoms: A route that fails remains in the routing table with its old metric, preventing an alternate route from being used and causing a routing loop.

  Conditions: This symptom is observed in a network that is configured for IS-IS and iSPF when the IP routes that are advertised in a fragmented LSP do not age-out during a rerouting failure.

  Workaround: Remove iSPF from the IS-IS process by entering the **router isis** command followed by the **no ispf** command.

- CSCsa82134

  Symptoms: A router that is configured for IS-IS may reload unexpectedly.

  Conditions: This symptom is observe on a Cisco router when there are more than 64 equal-cost next hops for an IPv6 route that is learned from IS-IS.

  Workaround: There is no workaround. However, the conditions are unlikely to occur in a production network.

Miscellaneous

- CSCdz18851

  Symptoms: When you reload microcode onto a line card or perform an OIR of a line card, a spurious memory access error may be logged on some or all other line cards in the router.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 dCEF when an IPv6 route is loadbalanced across two equal cost paths that both leave the router on interfaces of the same line card, which is the line card onto which you reload microcode or on which you perform an OIR.

  Workaround: There is no workaround.

- CSCed68627

  Symptoms: A spoke-to-spoke tunnel fails to come up over a secondary tunnel interface, causing spoke-to-spoke traffic to traverse the secondary hub router.

  Conditions: This symptom is observed in a Dual Hub Dual Dynamic Multipoint VPN (DMVPN) configuration when there is already a dynamic spoke-to-spoke tunnel over a primary tunnel interface and when the primary hub router becomes unavailable.

  Workaround: There is no workaround. We recommend that you use the Dual Hub Single DMVPN network configuration, in which the symptom does not occur.

  Further Problem Description: In order for the fix of this caveat to work, if you have tunnels that use the same tunnel source, then you must use "shared" tunnel protection and you must use an interface (as opposed to an IP address) as the tunnel source.

- CSCed83044

  Symptoms: A standby RSP may reload with the following error message:

  ```
  %SYS-6-STACKLOW: Stack for process IPC Seat Manager running low
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(27)S with IOPS when RPR, RPR+ or SSO redundancy modes are configured and when certain ATM subconfiguration commands such as the **connect** command are executed on the active RSP. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed94829

  Multiple Cisco products contain vulnerabilities in the processing of IPSec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for IPSec and can be repeatedly exploited to produce a denial of service.

  Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

  This advisory is posted at

  http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml.

- CSCee25478

  Symptoms: A PVC-in-range configuration is lost after an OIR of a line card.

  Conditions: This symptom is observed only when create on-demand PVCs are configured.

  Workaround: There is no workaround.

- CSCee31450

  Symptoms: IPv6 packets may not be switched via CEFv6 but may be blackholed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S4 when the packets are switched from an FE interface to a POS interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee42660

  Symptoms: The following error message may be generated when you change a PVC to a different class VC with a different UBR+ speed, the PVC may then enter a block state, and the router may eventually crash:

```
%ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=<>,VPI=<>, VCI=<>) on Interface <>,
(Cause of the failure: PVC removal during recreation failed)
```

Conditions: This symptom is observed on a Cisco router that has an Auto VC and PVC-in-range configuration.

Workaround: There is no workaround.

- CSCef81634

  Symptoms: When you bring up and tear down SSG sessions quickly, a router may crash because of a bus error exception.

  Conditions: This symptom is observed on a Cisco router that is configured for SSG when you use a tool that initializes the interface and quickly brings sessions back up while the old sessions are still being cleared.

  Workaround: There is no workaround.

- CSCef84174

  Symptoms: PPP forwarding may fail between two virtual access interfaces.

  Conditions: This symptom is observed on a Cisco AS5850 but is not platform-dependent.

  Workaround: Disable PPP multilink on the asynchronous interfaces.

- CSCeg02918

  Symptoms: A Cisco router that is configured with an HTTP authentication proxy may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a crypto image of Cisco IOS Release 12.3(9) or Release 12.3(10).

  Workaround: Disable the HTTP authentication proxy. If this is not an option, there is no workaround.

- CSCeg23300

  Symptoms: When you enter the **show memory** *address* command, irrespective of whether or not you place an optional keyword after the pipe (vertical bar), the console or vty session hangs and cannot be restored without reloading the platform. This situation especially impacts the console, but as long as there is a vty session available, Telnet still functions.

  Although the platform may return the initially requested data, it does not return the prompt. The session (either console logging and/or terminal monitoring) continues to generate system or error messages to the terminal.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series but is platform-independent.

  Workaround: Reload the platform. The stalled prompt will eventually recover but this could take many hours or even days.

  Further Problem Description: The symptom is expected behavior because the parser must scan the entire range of possible (and ever growing) memory addresses. For this reason, we recommend against the use of the **show memory** *address* command, which will be removed from common usage in all future releases.

- CSCeg23873

  Symptoms: Authorization does not function for mobile IP subscribers.

  Conditions: This symptom is observed when TACACS+ is configured for authorization.

  Workaround: Configure RADIUS for authorization or configure the security associations locally.

- CSCeg32227

  Symptoms: ATM VC output tail drops occur on a Cisco MGX 8800 series RPM-XF. Resource error drops increase for resource number 6 or 7.

  Conditions: This symptom is observed when the outgoing traffic is more than what the ATM VCs can handle. The Cisco MGX 8800 series RPM-XF has a FPGA revision of less than 16.

  Workaround: Police the outgoing ATM traffic.

- 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.

- CSCeg59749

  Symptoms: There is no end-to-end DTMF path confirmation.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 2800 series when a SIP media-forking call is made.

  Workaround: There is no workaround.

- CSCeg65615

  Symptoms: A Cisco router may crash when the ATM class of services is changed or when an ATM interface is shut down while traffic is running over the interface.

  Conditions: This symptom is observed rarely when the ATM class of services is changed for an ATM PVC on a DSL ATM interface. The symptom may affect the following routers if they are configured with a DSL WIC: Cisco 1700 series, Cisco 1800 series, Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.

  Workaround: Before you change the ATM class of services or before you shut down the ATM interface, stop the traffic on the interface.

- CSCeg74233

  Symptoms: Some packet data protocol (PDP) contexts may not be deleted from a gateway GPRS support node (GGSN).

  Conditions: This symptom is observed when an error occurs while PDP contexts are waiting for a delete response.

  Workaround: If the PDP context exist in the Serving GPRS Support Node (SGSN), delete the PDP context from the SGSN. If the PDP context does not exist in the SGSN, there is no workaround.

- CSCeh08363

  Symptoms: Bidirectional DTR does not function. The output of the **show dialer** command shows the incorrect dialer type.

  Conditions: This symptom is observed on a Cisco 3660 that runs Cisco IOS interim Release 12.3(12.9)T.

  Workaround: There is no workaround.

- CSCeh09198

  Symptoms: A Cisco gateway that has the garbage detector (a tool that is used for debugging memory leaks) enabled may hang indefinitely.

Conditions: This symptom is observed when you enter the garbage detector-related **show memory debug leaks** command or **show memory debug incremental leaks** command.

Workaround: There is no workaround.

- CSCeh32332

  Symptoms: RIP removes the interface information for an interface that has the **ip unnumbered** command enabled from the RIP database when another interface that has the **transmit-interface** command enabled goes down.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(12a).

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that has the **ip unnumbered** command enabled.

- CSCeh40161

  Symptoms: When a branch router attempts to access the Internet via HTTP or TCP, the HTP or TCP session times out unexpectedly.

  Conditions: This symptom is observed when the router at the headquarter has a Cisco IOS Firewall and resets the HTTP or TCP connection.

  Workaround: Configure a GRE+IPSec connection between the branch router and the router at the headquarter.

  Alternate Workaround: Disable the Cisco IOS Firewall on the router at the headquarter.

- CSCeh47169

  Symptoms: A Cisco router may reload because of I/O memory corruption when you use Telnet, reverse Telnet, rsh, or other vty-based applications, for example, a vty-based application to access a service module.

  Conditions: This symptom is observed on a Cisco 2851, Cisco 3745, and Cisco 3845 that contain the fix for caveat CSCef84400.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef84400. 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.

- CSCeh55603

  Symptoms: The PXF engine on a Cisco 8800 series MGX RPM-XF crashes and an error message similar to the following is generated:

  ```
  %PXF-2-FAULT: T0 XCM2 Address Error: R1
  ```

  The address error may also be R2, R3, and so on.

  Conditions: This symptom is observed when there is bidirectional traffic that is either compressed or uncompressed by means of cRTP, IPHC, or TCP compression configurations.

  Workaround: There is no workaround. However, after the crash, the PXF engine reloads and recovers by itself.

- CSCeh56264

  Symptoms: The PXF engine of a Cisco MGX 8800 series RPM-XF may crash because of a TBB length error.

  Conditions: This symptom is observed when the Cisco MGX 8800 series RPM-XF processes a packet that causes a TBB length error.

Workaround: There is no workaround. Note that the PXF engine reloads automatically but there is short outage when the hardware forwarding is disabled.

- CSCeh56402

  Symptoms: A router may crash when you shut down the Frame Relay interface of a peer.

  Conditions: This symptom is observed on a Cisco router that connects to the peer via a serial interface that has Frame Relay encapsulation and encryption enabled.

  Workaround: There is no workaround.

- CSCeh61467

  This caveat consists of the two symptoms, two conditions, and two workarounds:

  6. Symptom 1: After you have disabled MVPN on a VRF interface, the CPU use for the PIM process increases to 99 or 100 percent and remains at that level.

     Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases.

     Workaround 1: Before you disable MVPN on the VRF interface, enable and then disable multicast routing by entering the **ip multicast-routing vrf** *vrf-name* global configuration command followed by the **no ip multicast-routing vrf** *vrf-name* global configuration command.

  7. Symptom 2: A router that functions under stress and that is configured with a VRF interface may crash when an MDT group is removed from a remote PE router.

     Condition 2: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases, and occurs only when there are frequent link flaps or other multicast topology changes that affect the VRF interface.

     Workaround 2: There is no workaround.

- CSCeh63526

  Symptoms: A router crashes at the “insp_inspection” function.

  Conditions: This symptom is observed when the inspection rule is removed and re-added to an interface while traffic passes through the interface.

  Workaround: There is no workaround.

- CSCeh76209

  Symptoms: When Policy Based Routing (PBR) is configured with the **set interface** command, packets continue to be forwarded to an interface when that went down, causing packets to be dropped. When the **ip local policy route-map** command is enabled, all locally-generated packets are impacted.

  Conditions: This symptom is observed on a Cisco router and only applies to packets that require process-switching.

  Workaround: Do not enter the **set interface** command. Rather, enter the **set ip next-hop** command.

- CSCeh88604

  Symptoms: One or more VIP slot controllers reset.

  Conditions: This symptom is observed on a Cisco 7500 series when the **ip nbar protocol-discovery** command is enabled. The symptom may not be platform-dependent and may also occur on other platforms in a similar configuration.

  Workaround: Disable protocol discovery by entering the **no ip nbar protocol-discovery** command.

- CSCeh90322

  Symptoms: Calls do not go through because of incompatibility between a Cisco gateway and a third-party vendor gateway.

  Conditions: This symptom is observed on a Cisco 7200 series that is connected to a Cisco gateway running H.323 version 4 that, in turn, is connected to a third-party vendor gateway running H.323 version 2.

  H.323 version 4 messages include "User-User" as a mandatory element but H.323 version 2 messages do not. This situation affects SetupAcknowledge, Status, StatusInquiry, and Notify messages, and prevents calls from being properly set up.

  Workaround: There is no workaround.

- CSCeh93087

  Symptoms: When an RPF change occurs, a bidirectional PIM convergence may take up to 10 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series but is platform-independent.

  Workaround: There is no workaround.

- CSCeh95160

  Symptoms: When a unicast routing update occurs during the DF election process, the DF winner may receive an incorrect metric.

  Conditions: This symptom is observed on a Cisco router that is configured for bidirectional PIM.

  Workaround: Clear the DF on the winning router and trigger another DF election.

- CSCeh95801

  Symptoms: The domain name does not appear in the accounting records.

  Conditions: This symptom is observed when EzVPN clients use digital certifications that are terminated on a Cisco router and when RADIUS accounting is enabled.

  Workaround: Use the accounting information that is available such as the Group-ID.

- CSCeh96861

  Symptoms: One-way audio or no audio may occur during a call that is made through a Cisco AS5400.

  Conditions: This symptom is observed when the Cisco AS5400 functions as a terminating gateway and is connected to a Cisco 3600 series or Cisco 3800 series that functions as an originating gateway. All platforms run Cisco IOS Release 12.3(14)T. The symptom may also occur in later releases.

  Workaround: Enter the **playout-delay nominal 200** command on the voice port that is used for the call.

- CSCei00735

  Symptoms: A call may fail and the output of the **debug mgcp packet** command may show the following error:

  ```
  500 2157190 Endpoint database internal error
  ```

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that are configured with an NM-HDV2 network module when the following conditions are present:

  - The controllers of an NM-HDV2 network module are configured for CAS.
  - MGCP is used for voice call control.

  - Controller 1/0/0 is configured before controller 1/0 is configured or controller 1/0/1 is configured before controller 1/1 is configured, either on the gateway or on the call manager.

  Workaround: Configure the controllers in the order that is listed in the output of the **show running-config** command. Specifically, in the order 1/0, 1/1, 1/0/0, 1/0/1, both on the gateway and the call manager.

- CSCei02275

  Symptoms: A Cisco router may reload when removing a Frame Relay map from a dial interface.

  Conditions: This symptom occurs when a dial (ISDN) interface is configured for Frame Relay encapsulation with a map that includes IP Header Compression.

  Workaround: There is no workaround.

- CSCei02787

  Symptoms: A management gateway on which IPSec HA is configured leaks memory, eventually causing the gateway to reload when it drains out of all memory.

  Conditions: This symptom is observed on a Cisco platform that functions as a gateway and that processes IKE sessions.

  Workaround: There is no workaround.

- CSCei05708

  Symptoms: You cannot enable or disable the Visual Message Waiting Indicator (VMWI) of an analog phone via an MCGP call manager.

  Conditions: This symptom is observed when the analog phone is connected to a Cisco router that runs a Cisco IOS software image that supports the Distributed Stream Media Processor (DSMP).

  Workaround: There is no workaround.

- CSCei08347

  Symptoms: When you ping a Gigabit Ethernet (GE) interface on an NPE-G1 that has the **ip pim sparse-mode** or **ip pim sparse-dense-mode** command enabled, the ping fails.

  Conditions: This symptom is observed on a Cisco 7200 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the GE interface of the NPE-G1.

  Workaround: After you have shut down and brought up the GE interface, enter the **no ip pim sparse-mode** or **no ip pim sparse-dense-mode** command and then reconfigure the command.

- CSCei08458

  Symptoms: The FIB may be disabled or the output interface may be stuck on an A3 ATM port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dLFIoATM.

  Workaround: Reload the microcode or perform an OIR to recover the A3 ATM port adapter.

- CSCei09099

  Symptoms: When you boot a router, the following error message and traceback are generated:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 64ED6DD0.
  -Process= "Crypto IKMP", ipl= 4, pid= 181
  -Traceback= 0x606DE040 0x607EC260 0x607F3264 0x62799FFC
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for ISAKMP.

  Workaround: There is no workaround.

- CSCei09130

  Symptoms: A Cisco 2600XM series that is configured with an AIM module may increment layer 1 errors and clock slips.

  Conditions: This symptom is observed only on a Cisco 2600XM series that runs Cisco IOS Release 12.4 when the following four specific conditions occur:

  - The router is configured with an AIM-ATM, AIM-VOICE, or AIM-ATM-VOICE module.
  - The router is configured with a VWIC-2MFT-x card. (The symptom does not occur with a VWIC-1MFT-x card.)
  - Both ports of the VWIC-2MFT-x card are configured for Line Timing.
  - The first VWIC port is connected and active, while the second VWIC port is either disconnected, in the LOS alarm state, or on a different clock domain than the first VWIC port.

  The symptom could also occur on a Cisco 2600XM series that runs Release 12.4 or Release 12.4.T.

  Workaround: There is no workaround.

- CSCei09876

  Symptoms: A router that is configured for MPLS VPN cannot accept a Route Distinguisher with the value 0:0.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.4 and that integrates the fix for CSCeh12594. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh12594. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Use a Route Distinguisher with another value. If this is not an option, there is no workaround.

- CSCei18172

  Symptoms: When a service policy with a drop action is attached to multiple subinterfaces and then removed from one of the subinterfaces, the other subinterfaces stop applying drop actions.

  Conditions: This symptom is observed on a Cisco router when a service policy with a drop action is attached to multiple subinterfaces of the same main interface.

  Workaround: Re-add the service policy to the other subinterfaces.

- CSCei19478

  Symptoms: You cannot load all STRING.UDP signatures.

  Conditions: This symptom is observed on a Cisco platform that is configured for IPS.

  Workaround: There is no workaround.

- CSCei21134

  Symptoms: A Cisco MGX 8800 series RPM-XF does not monitor the queue size allocation to VCs to ensure that SAR buffer oversubscription does not occur.

  Conditions: This symptom is observed when VC queue-depth and CoSQ queue-limit values are configured to override default queue sizes.

  Workaround: There is no workaround.

- CSCei21355

  Symptoms: A Cisco AS5850 reloads unexpectedly with a traceback while voice calls and fax calls are brought up simultaneously.

Conditions: This symptom is observed when you bring up more than 500 SIP and H.323 voice calls and 92 T.38 Fax Relay calls.

Workaround: Bring up voice calls only; do not bring up fax calls.

- CSCei22930

  Symptoms: When link flaps occur while a bandwidth change takes place, the QoS configurations are ignored and deleted from an ATM interface that is configured with an IMA group, and the following error messages and tracebacks are generated:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  -Traceback= 611D46E8 6002160C 61D4EF90 602C329C 602C6574 602C6D40 61D52170 61D54F2C
  61D553E8 61D55784 61D6FF84 61D550EC 61D5516C 604818FC 6047E89C 6047E9C8

  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
  -Traceback= 611D46E8 600177F4 6145DCB4 6145DDFC 6146B8E8 6146E174 616AB8B0 616ABB58
  6205C598 62066DE0 6205C640 61D557F0 61D6FF84 61D550EC 61D5516C 604818FC

  %SYS-2-MALLOCFAIL: Memory allocation of 19 bytes failed from 0x6145DCAC, alignment 0
  Pool: Processor  Free: 139749528  Cause: Interrupt level allocation
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
  -Process= "<interrupt level>", ipl= 1, pid= 3
  -Traceback= 611D46E8 60012958 6001822C 6145DCB4 6145DDFC 6146B8E8 6146E174 616AB8B0
  616ABB58 6205C598 62066DE0 6205C640 61D557F0 61D6FF84 61D550EC 61D5516C
  ```

  Conditions: These symptoms are observed on a multiport T1/E1 ATM network module with IMA when the ATM interface is configured with an IMA group, has the **atm bandwidth dynamic** command enabled, and is configured for QoS.

  Workaround: Enter the **bandwidth** command on the ATM interface that is configured with an IMA group to define the total bandwidth for all UNI interfaces of that IMA group.

  Alternate Workaround: Do not configure the **atm bandwidth dynamic** command when the ATM interface is configured with an IMA group and QoS.

- CSCei23159

  Symptoms: The HSRP feature does not work on NM-16/36ESW ports configured as L3 routed ports through the **no switchport** command. HSRP works correctly on the VLAN interface and onboard L3 interfaces of the router.

  Conditions: This symptom has been observed on all routers which use NM-16/36ESW.

  Workaround: Use either of the following workarounds as necessary:

  1. 1) Use the MAC address of the physical interface for the HSRP virtual MAC address, but this could not be applied in customer's design.

  or

  2. 2) Enable the **standby use-bia** command under the Routed Interface as in the following example:

  ```
  interface FastEthernet1/0
   no switchport
   ip address 10.116.216.2 255.255.255.0
   standby use-bia
   standby 2 ip 10.116.216.1
   standby 2 preempt
  end
  ```

- CSCei23461

  Symptoms: When you reboot a router that is configured with an NM-32A network module, a software-forced crash may occur.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T. When you remove the cabling from the NM-32A network module, the router boots without any problem.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(8)T6.

- CSCei24086

  Symptoms: A Cisco AS5850 gateway that processes mixed traffic reloads unexpectedly after a few minutes of functioning under stress.

  Conditions: This symptom is observed on a Cisco AS5850 gateway that runs Cisco IOS interim Release 12.4(1.8)T and that is configured with voice traffic (H.323 and SIP) with PRI and CAS, Fax Relay T.38, and TDM Hairpinning.

  Workaround: There is no workaround.

- CSCei27330

  Symptoms: A router that is configured for Dynamic Multipoint VPN (DMVPN) may frequently generate the following error message:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done
  ```

  Conditions: This symptom is observed on a Cisco router such as a Cisco 871 and Cisco 1800 series that function as a DMVPN spoke.

  Workaround: There is no workaround.

- CSCei28413

  Symptoms: A Cisco 3700 series that is configured for MGCP may crash because of a bus error and generate the following error message:

  ```
  System returned to ROM by bus error at PC 0x613F72D0, address 0xD0D0D15
  ```

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.4(1).

  Workaround: There is no workaround.

- CSCei31970

  Symptoms: When you enter the **show voice call status** *call-id* command several times in quick succession, the CPU use of a Cisco AS5850 reaches 99 percent and the Cisco AS5850 starts rejecting calls. The Cisco AS5850 thereafter becomes very unstable in accepting incoming calls. This situation can be highly service-impacting.

  Conditions: This symptom is observed on a Cisco AS5850 that runs a special image of Cisco IOS Release 12.3(11)T6 and occurs only when there are more than 900 H.323 voice calls.

  Workaround: Do not enter the **show voice call status** *call-id* command in a stress situation.

- CSCei32287

  Symptoms: The following message and traceback may be generated on a Cisco platform that is configured for Tcl:

  ```
  %SCHED-3-THRASHING: Process thrashing on watched message event.
  -Process= "Tcl Serv - tty0", ipl= 6, pid= 92 -Traceback= 0x8089D344
  0x8118E624 0x8118E6EC 0x810DC29C 0x805AACF8 0x805AE2B0
  ```

  Conditions: This symptom is observed when you enter and exit the Tcl shell rapidly, for example by cutting and pasting the following commands into the console:

  ```
  tclsh
  tclquit
  ```

  Workaround: Avoid entering the commands rapidly.

- CSCei33351

  Symptoms: A router that is configured for QoS crashes because of a bus error.

  Conditions: This symptom is observed when you bring up a session that has a policy map attached in both directions.

  Workaround: There is no workaround.

- CSCei33828

  Symptoms: A router that is being reloaded may not bring up all ATM VPs.

  Conditions: This symptom is observed on a Cisco 10000 series only when the **atm over-subscription-factor** command is enabled. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCei33881

  Symptoms: The following error message is generated when you attempt to configure tunnel protection on an IPIP tunnel:

  ```
  ERROR: tunnel protection is only valid on IPIP, GRE, and MGRE interfaces
  ```

  This situation prevents tunnel protection from functioning on an IPIP tunnel.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T or Release 12.4.

  Workaround: There is no workaround.

- CSCei36482

  Symptoms: The output of the **show resource user iosprocess brief** command does show the resource owner (RO) and its usage by resource user (RU) but only for the first RU. Starting from the second RU, the ROs are displayed incorrectly, that is, only the buffer RO is shown. Other RO information such as CPU use are not displayed.

  Conditions: This symptom is observed on a Cisco router that has the Embedded Resource Manager (ERM) enabled.

  Workaround: Do not enter the **show resource user iosprocess brief** command. Rather, enter the **show resource owner** command as in the following example: **show resource owner cpu user iosprocess**. The output of this command shows the CPU use for the RO for all RUs in the "iosprocess" Resource User Type (RUT). Note that the symptom does not impact the functionality of the ERM or the router.

- CSCei37015

  Symptoms: A router that is configured to use RSA signature authentication and that deploys certificates during IKE phase 1 crashes when you boot the router with a new image.

  Conditions: This symptom is observed on a Cisco 1721 when you boot the router with Cisco IOS Release 12.3(9d). However, the symptom is platform-independent. The crash occurs during the setup of the IKE SA.

  Possible Workaround: Disable IKE before you reload the router with the new image.

- CSCei37299

  Symptoms: A VPN hub router may reload when you enter the **clear crypto session remote** *ip-address* command.

  Conditions: This symptom is observed after a remote peer disconnects ungracefully (that is, the peer is suddenly powered-off or the LAN cable is disconnected) and immediately reconnects to the VPN hub router with a different public address.

Workaround: Do not enter the **clear crypto session remote** *ip-address* command. Rather, enter the **clear crypto sa** command.

- CSCei37769

  Symptoms: WRED threshold cell values may become undesirably high for a Cisco MGX 8800 series RPM-XF that is changed from a high-speed to a low-speed configuration.

  Conditions: This symptom is observed when a high-speed RPM-XF with output policy maps that have WRED classes with high packet thresholds is converted to a low-speed RPM-XF by configuring SAR-based CBWFQ. This situation causes a conversion of the thresholds from packets to cells.

  Workaround: Change the large cell thresholds manually to the appropriate values.

- CSCei38378

  Symptoms: A router that receives a Restart in Progress (RSIP) message for an individual endpoint does not select an alternate IP address.

  Conditions: This symptom is observed on a Cisco router that is configured for Voice XGCP.

  Workaround: There is no workaround.

- CSCei38409

  Symptoms: A Cisco router crashes during certificate enrollment.

  Conditions: This symptom is observed when certificate enrollment is performed manually.

  Workaround: Perform certificate enrollment by using Simple Certificate Enrollment Protocol (SCEP).

- CSCei40048

  Symptoms: A Cisco AS5400 may reload when it functions in an environment with a Cisco Customer Voice Portal (CVP) and Nuance Text-to-speech (TTS).

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS interim Release 12.4(2.2) and that functions under a stress load.

  Workaround: There is no workaround.

- CSCei40059

  Symptoms: Ping fails after you enter the **ip cef accounting** interface configuration command.

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-XF that is configured for MPLS VRF.

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

- CSCei41674

  Symptoms: A router may generate “SYS-2-LINKED: Bad enqueue” error messages.

  Conditions: This symptom is observed when both the following conditions are present:

  – The router generates traffic such as routing updates that are encrypted via IPSec and the traffic (packets) is process-switched after encryption.

  – The router is configured with a hardware crypto accelerator.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CCSCeg43855. 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: When the error message is generated, a crash may also occur in the following configuration in which hub-n-spoke GRE tunnels are configured for IPSec and EIGRP: When the spokes have a primary hub and a backup hub (that is, a GRE tunnel to each) and when a switchover from the primary hub to the backup hub occurs multiple times, the spoke man crash. This particular situation is observed on a Cisco 1841 and Cisco 3825.

A workaround for this particular situation is to prevent multiple hub switchovers from occurring or to refrain from configuring GRE tunnels with IPSec and EIGRP.

- CSCei42842

  Symptoms: A Cisco 2851 may crash at the "tsp_search_voice_port" function.

  Conditions: This symptom is observed when the **no ccm-manager mgcp** command is entered very rapidly, for example, via an automated script.

  Workaround: There is no workaround.

- CSCei45749

  Symptoms: When you enter the **clear interface** command on an Inverse Multiplexing for ATM (IMA) interface configured for dynamic bandwidth, the PVCs that are associated with the IMA interface may become Inactive.

  Conditions: This symptom is observed only for IMA interfaces that have the **atm bandwidth dynamic** command enabled.

  Workaround: Issuing the command **no atm bandwidth dynamic** from the IMA interface can prevent the problem from happening. If the problem has been experienced already, using the command **no atm bandwidth dynamic** followed by a **shutdown** and subsequent **no shutdown** from the IMA interface can be used to workaround the problem and clear the inactive PVC condition.

- CSCei46472

  Symptoms: A traceback is generated at the tcatmTagVCSendWithdraw function, causing the router to reload because of a software-forced crash.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(3.9)T1 and that is configured for MPLS LSC. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCei46509

  Symptoms: No more than 930 H.323 terminating calls can be brought up on a Cisco 5850 because socket allocation failures occur.

  Conditions: This symptom is observed on a Cisco 5850 that functions as a TGW in RPR+ mode when H.323 slow start is enabled and when H.245 tunneling is disabled. Note that the symptom does not occur when H.245 tunneling is enabled or when the Cisco 5850 functions as an OGW.

  Workaround: Configure H.245 tunneling and fast start by entering the following commands:

  ```
  Router(config)# voice service voip
  Router(conf-voi-serv)#h323
  Router(conf-serv-h323)#no h245 tunnel disable
  ```

- CSCei46978

  Symptoms: A Cisco 7200 series may generate the following error message, and links flap:

  ```
  %SBETH-3-ERRINT: GigabitEthernet0/1, error interrupt, mac_status = 0x0000000000840000
  ```

Conditions: These symptoms are observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(15) and that is configured with an NPE-G1.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(13).

- CSCei49745

  Symptoms: A router may crash when a certificate is revoked by entering the **crypto pki server** *cs-label* **revoke** *certificate-serial-number* command.

  Conditions: This symptom is observed on a Cisco switch or router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCei50425

  Symptoms: A Cisco 7200 series or Cisco 7301 that is equipped with a VAM, VAM2 or VAM2+ accelerator may refuse a valid RSA key and generate an error message such as the following:

  ```
  % Error in generating keys: did not validate % Key pair import failed.
  ```

  Conditions: This symptom is observed under rare circumstances when a valid RSA key is composed of unusually short or long prime numbers and coefficient.

  When the VAM is deactivated during the importation of the RSA key, the router accepts the key but when the VAM, VAM2, or VAM2+ is inserted into the chassis, the router miscomputates the signature payload of the IKE/ISAKMP exchanges.

  Workaround: Create a new RSA key.

  Further Problem Description: The result of the wrong operation can be seen on the other side of the connection by activating the **debug crypto engine** and **debug crypto isakmp** commands. The following messages are related to the failure:

  ```
  crypto_engine: public key verify
  crypto_engine: public key verify, got error no available resources
  ISAKMP:(0:2:HW:2): signature invalid!
  ```

- CSCei51142

  Symptoms: A CA server that is rebooted may reset the issued serial number to 1, thus re-issuing a certificate with the same serial number.

  Conditions: This symptom is observed on Cisco routers such as a Cisco 1841 and Cisco 2811 that have a built-in hardware clock.

  Workaround: There is no workaround.

- CSCei51322

  Symptoms: A router that is configured for IPSec may reload because of a stack or program counter corruption.

  Conditions: This symptom is observed on a Cisco router that uses a certificate with a very long subject name of several hundred bytes when the distinguished name (DN) is used as an ISAKMP identity. The symptom does not occur for shorter subject names (for example, 290 characters). In most environments, a subject name of 80 characters or less is common.

  Workaround: Use certificates with a shorter subject name.

- CSCei52380

  Symptoms: The entry for a tunnel is missing from the mplsOutSegmentTopLabel column of the MPLS-LSR-MIB.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when a mibwalk is performed on the mplsOutSegmentTopLabel object.

Workaround: There is no workaround.

- CSCei52546

  Symptoms: The **atm-ldp** keyword in **show mpls** commands is not recognized.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that is configured with an RSP and that run Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCei56682

  Symptoms: A Cisco AS5400 cannot perform outbound signaling for Feature Group D Operator Services (FGD-OS).

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.3T, Release 12.4, or Release 12.4T.

  Workaround: There is no workaround.

- CSCei59221

  Symptoms: Traffic does not pass over a connection between a Cisco AXSM-XG module and a Cisco MGX 8800 series RPM-XF after a graceful hardware migration of a redundant pair of AXSM/A, AXSM/B, or AXSM-E cards to AXSM-XG cards.

  Conditions: This symptom is observed after the hardware migration for the connections that already existed between the AXSM/A, AXSM/B, or AXSM-E card and the RPM-XF before the hardware migration. The symptom does not occur for new connections that are added between the AXSM-XG and the RPM-XF after the hardware migration, nor does the symptom occur for hardware migrations of standalone (as opposed to redundant pairs of) AXSM/A, AXSM/B, or AXSM-E cards to AXSM-XG cards.

  Workaround: After the hardware migration, delete and re-add the affected connections.

- CSCei61814

  Symptoms: A Fast Ethernet (FE) interface on a Cisco AS5850 may reset unexpectedly.

  Conditions: This symptom is observed when you attempt to program the FE controller for multicast or broadcast traffic such as OSPF, EIGRP, RIP, or PIM.

  Workaround: There is no workaround.

- CSCei62348

  Symptoms: A Cisco 2691 crashes because of a bus error exception and alignment errors.

  Conditions: This symptom is observed when SNMP passes invalid VLAN IDs to VTP.

  Workaround: There is no workaround.

- CSCei62952

  Symptoms: After the PXF engine crashes or reloads, some prefixes are no longer routable.

  Conditions: This symptom is observed on a Cisco router after the PXF engine crashes or after you have entered the **microcode reload pxf** command.

  Workaround: Initiate an RP switchover or reboot the router.

- CSCei66542

  Symptoms: SGBP AAA authentication fails in a large scale dial-in configuration.

Conditions: This symptom is observed when a bid is processed and when an incorrect name is retrieved, causing an incorrect user name to be sent and the AAA authentication to fail.

Workaround: There is no workaround.

- CSCei69551

  Symptoms: When a router is reloaded, the E lead (input) on an E&M port is seized for a duration of 20 to 25 seconds, causing a radio system that is connected to the E&M port to be activated.

  Conditions: This symptom is observed in a Cisco Land Mobile Radio (LMR) configuration when you enter the **bootup e-lead off** command.

  Workaround: There is no workaround.

- CSCei70222

  Symptoms: All IKE IPSec SAs are down and encryption services do not function when an hardware encryption engine is enabled.

  Conditions: This symptom is observed on a Cisco router that is configured with a VAM, VAM2, or VAM2+ when the router runs under low memory conditions.

  Workaround: There is no workaround. Reboot the router to temporarily resolve the symptoms.

  Further Problem Description: When the **debug crypto engine error** command is enabled, the following debug message is generated:

  ```
  CryptoEngine: epa_get_blk_buffer FAILED
  ```

- CSCei72576

  Symptoms: The following error message and traceback are generated on a Cisco MGX 8800 series RPM-XF, and you cannot ping a destination:

  ```
  %GENERAL-3-EREVENT:HWCEF: Failed to alloc Mtrie HW node
  -Traceback= 4005B148 4005C398 4005C918 40066B5C 4028D634 4028DF6C 40294B84 4029AC5C
  4063D470 40614C90
  ```

  Conditions: This symptom is observed when there are many summary routes advertised with continuos route updates and withdraws via BGP or IGP sessions. The symptom occurs because the PXF CEF memory for level 4 becomes exhausted.

  Workaround: There is no workaround.

- CSCei75294

  Symptoms: A Cisco AS5850 that functions in RPR+ mode reloads unexpectedly because for each call an MGCP application holds an increasing amount of memory that is not freed up.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(11)T7. The symptom could also occur in Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCei75623

  Symptoms: A Cisco router may not forward multicast traffic that is has received via a GRE tunnel that belongs to a VRF.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4(2)T when CEF is enabled on the tunnel interface. The symptom does not occur with unicast traffic.

  Workaround: Disable CEF on the tunnel interface.

- CSCei77461

  Symptoms: A Cisco IAD2430 crashes when a connection trunk is configured on the onboard FXS voice port.

  Conditions: This symptom is observed when the connection trunk comes up after you have entered the **shutdown** command followed by the **no shutdown** command on the onboard FXS voice port.

  Workaround: There is no workaround.

- CSCei78391

  Symptoms: A VPN client stops receiving traffic from an IPSec gateway.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T but may also occur in Release 12.4 or Release 12.4T in the following topology:

  ```
  VPN client---NAT router---public cloud---2 IPSec HA gateways---inside subnet
  ```

  The symptom occurs when, after a Stateful Switchover (SSO), one of the IPSec gateways wrongly swaps the source and destination UDP ports that are used to return traffic to VPN client. This situation prevents the NAT router from finding the correct NAT entry, and, in turn, prevents the VPN client from receiving traffic form the IPSec gateway.

  Workaround: There is no workaround.

- CSCei79855

  Symptoms: When Cisco IOS software is secured using “secure boot” commands and after formatting the disk, the **show disk** command will not display the secured image and the corresponding configurations in the output.

  Conditions: This symptom occurs when securing the Cisco IOS software using the **secure boot-config** and the **secure boot- image** commands and formatting the disk.

  Workaround: There is no workaround.

- CSCei83160

  Symptoms: PIM neighbors do not recognize each other via a VRF tunnel interface because multicast does not receive MDT updates from BGP. The output of the **show log** command shows the following debug message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (3) received in update for prefix
  2:55:1111:192.168.31.1/32 from 192.168.31.1
  ```

  Conditions: This symptom is observed on a Cisco router and is not platform-dependent. The symptom occurs when a VRF instance is configured with BGP as the Exterior Gateway Protocol (EGP).

  Workaround: There is no workaround.

- CSCei83684

  Symptoms: WIC modules that have authentication enabled are not recognized.

  Conditions: This symptom is observed only on a Cisco IAD2430.

  Workaround: There is no workaround.

- CSCei86192

  Symptoms: When a buffer leak occurs, the RP crashes because of the starvation of buffers.

  Conditions: This symptom is observed on a Cisco 7500 series that has a VIP in which a channelized T1/E1 port adapter is installed and on Cisco 7600 series that has a FlexWAN in which a channelized T1/E1 port adapter is installed.

  Workaround: There is no workaround.

- CSCei93090

  Symptoms: EIGRP does not learn routes when the **ip pim sparse-dense-mode** command is configured on a Gigabit Ethernet interface.

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS interim Release 12.4(4.3).

  Workaround: There is no workaround.

- CSCej10160

  Symptoms: A spurious memory access is generated on a Cisco 3700 series, causing IPMC voice traffic to be dropped temporarily.

  Conditions: This symptom is observed on a Cisco 3700 series that has DSP-related features enabled and that has Cisco Land Mobile Radio (LMR) features configured on the voice ports.

  Workaround: There is no workaround.

- CSCej21891

  Symptoms: A router may crash when the **default-information originate** command is configured under the **router rip** command.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP.

  Workaround: Manually define a static default route and configure static redistribution under the **router rip** command.

- CSCej35355

  Symptoms: A voice port remains in the S_OPEN_PEND state, preventing a trunk from coming up.

  Conditions: This symptom is observed on a Cisco 2600 series when the voice port is configured via a T1 controller. The symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCin49358

  Symptoms: When an RSP switchover occurs on a Cisco 7500 series that functions in RPR+ mode, the SONET controller of a 1-port multichannel STM-1 port adapter does not come up after the switchover is complete. The output of the **show sonet controller** command shows that the controller status of the newly active RSP is down.

  Conditions: This symptom is observed when a switchover of the RSP occurs, either because of a failure on the active RSP or because of a forced switchover that occurs when you enter the **redundancy force-switchover rsp-standby-2-active** command.

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

- CSCin78416

  Symptoms: After a router has reloaded, unconfigured point-to-point (P2P) subinterfaces re-appear in the running configuration.

  Conditions: This symptom is observed when the **range** command is configured on a P2P subinterface and when member PVCs that are associated with the range do not receive traffic after the router has reloaded. The corresponding P2P subinterfaces of the member PVCs re-appear in the running configuration.

  Workaround: There is no workaround.

- CSCin78631

  Symptoms: A “PVC creation failure” error message is generated when a PVC that is part of a range is changed from an Auto VC to a normal VC.

  Conditions: This symptom is observed when a PVC range that is part of a point-to-point (P2P) subinterface is changed from an Auto VC to a normal VC.

  Workaround: Delete the range and reconfigure the range with normal VCs.

- CSCin78781

  Symptoms: An Auto VC remains inactive even through it receives traffic.

  Conditions: This symptom is observed when a VC class is configured on an Auto VC and when the parameters of the VC class are modified to trigger the re-creation of the PVC.

  Workaround: There is no workaround.

- CSCin78805

  Symptoms: VCs are inactive.

  Conditions: This symptom is observed when an Auto VC is configured as part of a range on a point-to-point (P2P) subinterface.

  Workaround: There is no workaround.

- CSCin79522

  Symptoms: A Cisco router that runs Cisco IOS Release 12.3T may reload when the ATM interfaces are swapped.

  Conditions: This symptom is observed when an ATM IMA port adaptor is removed and a PA-A3 port adaptor is inserted in the same slot and when there is at least one PVC configured that has the **inarp** enabled. The symptom may also occur in Release 12.3 or Release 12.4.

  Workaround: There is no workaround.

- CSCin85763

  Symptoms: A router hangs when T1 CAS is configured on the onboard T1 controller of an NM-HDV2-1T1/E1 and when you enter the **show voice trace 1/0:1.2** command, in which the “1” after the colon (“:”) represents the DS0 group number and the “2” represents the time slot that is traced.

  Conditions: This symptom is observed on a Cisco 3845 only when the time slot is included in the **show voice trace** command.

  Workaround: Do not include the time slot in the **show voice trace** command. For example, the router does not hang when you enter the **show voice trace 1/0:1** command.

- CSCin86322

  Symptoms: An end-to-end sweep ping fails across a dLFI bundle and the bundle flaps.

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

  Workaround: There is no workaround.

- CSCin93792

  Symptoms: A router crashes when you enter the **vpn service** *domain name* command.

  Conditions: This symptom is observed on a Cisco router that functions as a LAC when the *domain name* argument is longer than 210 characters.

  Workaround: There is no workaround.

- CSCin94279

  Symptoms: The “firewall are-u-there” feature on the Cisco EzVPN Client server does not support Cisco Security Agent (CSA).

  Conditions: This symptom has been observed on Cisco EzVPN Client servers.

  Workaround: There is no workaround.

- CSCin94305

  Symptoms: When the standby RSP on a Cisco 7500 series boots while a Versatile Interface Processor (VIP) or other interface processor on the router reloads, the standby RSP reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S, Release 12.2S, Release 12.2SB, Release 12.3T, Release 12.4, or Release 12.4T.

  Workaround: There is no workaround.

- CSCin94945

  Symptoms: A call setup fails when a transparent codec is configured for the incoming and outgoing dial peer of an IPIPGW.

  Conditions: This symptom is observed only for slow-start calls.

  Workaround: There is no workaround. Note that the symptom does not occur for fast-start calls.

- CSCin96402

  Symptoms: Confirmation fails in a test between a SIP gateway and an H.323 gateway with two IPIPGWs.

  Conditions: This symptom is observed in the following topology:

  ```
  [OGW]--[SIP]----[IPIPGW1]----[H323]----[IPIPGW2]----[SIP]--[TGW]
  ```

  The confirmation fails when the H.323 gateway is configured for fast start and has the **h245 tunnel disable** command enabled. The symptom does not occur when this command is not enabled. Also, when SIP debugs are enabled on the IPIPGWs and when the H.323 gateway is configured for fast start and has the **h245 tunnel disable** command enabled, calls do pass.

  Workaround: Do not configure the **h245 tunnel disable** command on the H.323 gateway.

  Alternate Workaround: Enable SIP debugs on the IPIPGWs.

- CSCin96617

  Symptoms: A router that has SSG enabled may refuse new incoming connections (either Telnet, PPP, or any type of AAA connection).

  Conditions: This symptom is observed when a very large amount of memory is held by SSG as a result of multiple IPCP negotiations for a PPP session.

  Workaround: There is no workaround.

- CSCsa41522

  Symptoms: A CPUHOG condition may occur when you delete an ATM subinterface on which a large VC group range is configured.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE2 and that runs Cisco IOS Release 12.3(7)XI1. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- CSCsa46484

  Symptoms: A VIP or FlexWAN module in which a PA-POS-2OC3 port adaptor is installed may crash.

  Conditions: This symptom is observed rarely and at random on a Cisco 7xxx series router or Cisco Catalyst 6000 series switch.

  Workaround: There is no workaround.

- CSCsa49177

  Symptoms: After you reload a router, the physical ATM interface for an IMA group interface remains down even though the T1 controllers are active.

  Conditions: This symptom is observed on a Modular Access Router such as a Cisco 3700 series that is configured with a VWIC-2MFT-T1 and an ATM-AIM.

  Workaround: Reload the router or remove and reconfigure all ATM parameters.

- CSCsa50067

  Symptoms: Modems do not longer dial after a few calls have been made. Rebooting the router temporary solves the problem until a few more calls have been made. The output of the **debug modem csm** command shows the following:

  ```
  Modem 3/1 CSM: (CSM_PROC_OC_CAS_WAITING_FOR_TONE)  <--DSX0_START_TX_TONE
  R2 Outgoing Modem(3/1): DSX (E1 1/0:17): STATE:
  R2_OUT_PROCESS_A R2 Got Event R2_START
  Modem 3/1 Mica: dialing number '#'
  Modem 3/1 CSM: (CSM_PROC_OC_CAS_WAITING_FOR_TONE)  <--ABORT_DIGIT_COLLECT
  Modem 3/1 CSM: (CSM_PROC_OC_CAS_WAITING_FOR_TONE)  <--MODEM_DIGITS_GENERATED
  ```

  Conditions: This symptom is observed on a Cisco 3745 that is configured with an E1 interface that uses R2 signaling. When you use reverse Telnet from the router to one of its modems, calls intermittently fail.

  Workaround: There is no workaround.

- CSCsa65819

  Symptoms: The Label Information Base (LIB) may not be disabled.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN when an IPv4 BGP neighbor that is configured to exchange MPLS labels goes down.

  Workaround: There is no workaround.

- CSCsa70040

  Symptoms: A router does not attempt to autoinstall a software configuration via a Frame Relay WAN segment when it receives a response to a DHCP request on an Ethernet LAN, even though the DHCP server does not support autoinstall via TFTP.

  Conditions: This symptom is observed when a software configuration is replaced on a failed remote router or installed on a new remote router. The router is connected to an existing Ethernet LAN and a Frame Relay WAN segment. You would expected that the router autoinstalls over the Frame Relay WAN segment because it is supposed to download the configuration from a central TFTP server. However, this does not occur.

  When the router has a response to its DHCP request on the Ethernet LAN, it attempts to autoinstall over DHCP. Although the DHCP server does not support autoinstall over DHCP, the router does not attempt to autoinstall over the Frame Relay WAN segment.

Workaround: Prevent the DHCP server from responding to the router's request or ensure that someone is physically present to disconnect the Ethernet LAN link from the router to force the router to autoinstall over the Frame Relay WAN segment. When the router has autoinstalled over the Frame Relay WAN segment, the router should be reconnected to the Ethernet LAN.

- CSCsa72313

  Symptoms: The following error messages may be generated on a router that has IP ACL enabled:

  ```
  %SYS-2-INSCHED: suspend within scheduler
  -Process= "<interrupt level>", ipl= 3
  -Traceback= 40525388 40628848 4060AED4 403F15BC 403F34F8 403F37EC 400901C8 4008E730
  406A0EEC 40621120
  ```

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7200 series, Cisco 7304, and Cisco 7500 series when a Turbo ACL compilation is configured along with an ACL on an ingress interface and when traffic passes through the ingress interface. The symptom does not affect the Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsa74930

  Symptoms: A Cisco 3825 or Cisco 3845 may display the following error message and traffic may be interrupted:

  ```
  %SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status = 0x0000000000840000
  ```

  Conditions: This symptom is observed when multiple users that are connected to a downstream switch attempt to log into network resources across a WAN that traverses the router. The symptom is most likely to occur when AppleTalk is configured over a Gigabit Ethernet connection.

  Workaround: There is no workaround.

- CSCsa82945

  Symptoms: A router crashes because of a bus error when ICMP or UDP packets that are larger than 1393 bytes are transmitted through an IPSec tunnel.

  Conditions: This symptom is observed when a policy map and crypto map are applied to the tunnel interface.

  Workaround: Remove the policy map.

- CSCsa86390

  Symptoms: A router generates an ALIGN-3-TRACE traceback and a DSPDUMP in its log, and the output of the **show align** command shows that the spurious access counter is not zero.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 2800 series when an error message is generated during stress calls.

  Workaround: There is no workaround.

- CSCsa86555

  Symptoms: The User Adaptation Layer for a Digital Private Network Signaling System (DPNSS) path does not come up.

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as a gateway and that run Cisco IOS Release 12.3(14)T or Release 12.4. The DPNSS path is configured on a VWIC-2MFT-E1-DI Multiflex Voice/WAN interface card that is installed in an NM-HDV2 network module.

  Workaround: There is no workaround.

- CSCsa86572

  Symptoms: A large configuration in NVRAM on a primary or secondary RSP may become corrupted and the router may generate relevant warning messages during the execution of a **copy system:running-config nvram: startup-config** command.

  When you erase NVRAM by entering the **erase nvram** command and then enter the **copy system:running-config nvram: startup-config** command, the router may crash.

  Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

  Workaround: If the configuration file is significantly large, place a copy of the configuration file on a flash card or disk with ample space and enter the **boot config slot0:startup-config** command to force the startup configuration file to be read from the flash card.

  When you enter the **copy system:running-config nvram: startup-config** command, the current running configuration is saved to the flash card or disk and the configuration is auto-synchronized to the corresponding flash card on the secondary RSP.

  Caution: Do not remove the flash card while the **boot config slot0:startup-config** command is being executed.

- CSCsa93207

  Symptoms: A Cisco 2600XM series that is configured with a WIC-1SHDSL-V2 WAN interface card (WIC) may crash.

  Conditions: This symptom is observed on a Cisco 2600XM series that runs Cisco IOS interim Release 12.4(1.6) and that runs a script that causes the WIC to be initialized in rate adaptive mode or auto mode. The symptom may also occur in Release 12.4T.

  Workaround: There is no workaround.

- CSCsa97663

  Symptoms: An ATM interface is unexpectedly removed from an IMA group even though the ATM interface is still in the up/up state, causing T1 links to be disconnected.

  Conditions: This symptom is observed on a Cisco 2600 series when you change the Cisco IOS software from Release 12.2(13)T8 to Release 12.3(12b).

  Workaround: Re-add the ATM interface to the IMA group by removing and reconfiguring the IMA configuration on the ATM interface.

- CSCsa97827

  Symptoms: A user who answers a call on a phone that is connected to an FXS port that has Calling Line ID (CLID) enabled for all voice gateways hears an audible squawk for a few seconds, followed by a normal media cut-through.

  Conditions: This symptom is observed on all voice gateways that run Cisco IOS Release 12.3(14) or a later release.

  Workaround: Wait for the analog phone to ring three or four times before you answer the phone.

- CSCsa99446

  Symptoms: A VoIP call is prematurely disconnected during a call hold period.

  Conditions: This symptom is observed on a Cisco platform that attempts to match the rotary dial peers.

  Workaround: There is no workaround.

- CSCsb01043

  Symptoms: When a Turbo ACL classification table grows beyond a certain size, a memory allocation failure may occur or the router may crash.

  If the router runs Cisco IOS Release 12.3, memory corruption may occur, causing the router to crash. If the router runs Cisco IOS Release 12.2S, an error message similar to the following may appear during a Turbo ACL compilation, the compilation will fail, and a recompilation is forced:

  ```
  %SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for TACL Block
  -Process= "TurboACL", ipl= 0, pid= 82
  ```

  These symptoms do not occur because of an out-of-memory condition.

  Conditions: This symptom is observed on a Cisco router that is configured for Turbo ACL. The Cisco 10000 series is not affected.

  Workaround: Monitor the output of the **show access-lists compiled** command and force the Turbo ACL tables to be cleared if a table is at risk of growing large enough to trigger the symptoms.

  The tables that have significant sizes are the first and third tables shown next to "L1:" and the first table shown next to "L2:". When the number after the slash for one of these tables is greater than 16384 for the "L1" tables or greater than 32768 for the "L2" table, the table is already too large and the symptom may occur any moment.

  When the number is in the range from 10924 to 16384 inclusive for the "L1" tables or the range from 21846 to 32768 inclusive for the "L2" tables, the table size will be too large on the next expansion. An expansion occurs when the number to the left of the slash reaches 90 percent of the value to the right of the slash. When the value to the left of the slash approaches 90 percent of the value to the right, enter the **no access-list compiled** command followed by the **access-list compiled** command to disable and re-enable Turbo ACL. Doing so causes the tables to be cleared and, therefore, delay the expansion. This workaround may be impractical when there is a high rate of incoming packets and when entries are added frequently to the tables.

  Alternative Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

  Note that neither of these workarounds are supported on a Cisco 7304 that is configured with an NSE-100: there is no workaround for this platform.

- CSCsb02061

  Symptoms: An "Output Hold Queue Wedge" condition may occur on PVCs that are defined on DS1 ports that are not configured for IMA.

  Conditions: This symptom is observed on a Cisco 7200 series that runs the c7200-ik9s-mz image of Cisco IOS Release 12.3(13), that is configured with a PA-A3-8T1-IMA port adapter that is configured for DSL aggregation, and that terminates hundreds of UBR VCs on a DS1 interface. The "Output Hold Queue Wedge" condition occurs on idle subinterfaces or when multiple point-to-point subinterfaces are "spawned" from a single subinterface by entering a PVC range command such as the following:

  ```
  interface ATM1/0.100 point-to-point
   ip unnumbered Loopback10
   atm route-bridged ip
   range pvc 6/100 6/599
  ```

  There are four workarounds:

  - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the physical interface.
  - Enter the **no pvc-in-range** command followed by the **pvc-in-range** command on a wedged VC.

  - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an uplink interface.
  - Tear down and rebuild a PVC.

- CSCsb04447

  Symptoms: A Cisco AS5400 does not generate a RADIUS stop record when a call disconnect is initiated by a modem on the Cisco AS5400.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.3(10a) or Release 12.3(12) and that is configured for PRI T1. The symptom does not occur when the remote end or a signal initiates the call disconnect.

  Workaround: There is no workaround.

- CSCsb07741

  Symptoms: Traffic with 0xA0 (precedence 5) is not classified as priority traffic and is placed in the best-effort class. When congestion occurs, this situation causes poor voice quality.

  Conditions: This symptom is observed when QoS is enabled on a Cisco Catalyst 6000 series Supervisor Engine 2.

  Workaround: Mark the packets on the originating gateway or disable QoS on the Supervisor Engine 2.

- CSCsb10341

  Symptoms: A Cisco 2651XM may not drop unicast Ethernet frames that are not destined for its MAC address.

  Conditions: This symptom is observed on a Cisco 3800 series that runs Cisco IOS Release 12.3(11)T5 or an earlier release or Release 12.3(14)T1 or an earlier release and that has subinterfaces that are configured for HSRP.

  Workaround: Enter the **standby use-bia** command on the main interface.

- CSCsb10711

  Symptoms: When you change the encapsulation on a Cisco router from X.25 to another encapsulation type, the router may reload and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x60A7AC24
  ```

  Conditions: This symptom is observed when TCP Header Compression is configured on an X.25 interface and the encapsulation is removed or changed, as, for example, in the following configuration:

  ```
  interface serial5/0
  ip address ip-address encapsulation x25
  x25 address x.121-address
  x25 map compressedtcp ip-address x.121-address
  x25 map ip-address x.121-address
  ```

  Workaround: Enter the **no x25 map compressedtcp** *ip-address x.121-address* command to remove the X.25 map before you change the encapsulation.

- CSCsb12405

  Symptoms: A fax call that is made over a VoIP MGCP link may fail when both the originating and terminating gateways have the **mgcp fax t38 gateway force** command enabled.

  Conditions: This symptom is observed on Cisco routers that run Cisco IOS Release 12.4 or interim Release 12.4(2.2)T.

Workaround: There is no workaround.

- CSCsb12516

  Symptoms: A router that is configured with IPSec tunnels may reload because of a software-forced crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- 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.

- CSCsb15582

  Symptoms: A PVC is unexpectedly removed from an IMA interface when one or more IMA links go down.

  Conditions: This symptom is observed on a Cisco router that has an ATM IMA interface that is configured with ATM dynamic bandwidth and no ATM oversubscription when you shut down one of the IMA links, causing dynamic bandwidth allocation to occur on the PVCs.

  Workaround: Reconfigure the PVCs with a bandwidth that can be supplied by the remaining IMA links.

- CSCsb16321

  Symptoms: The logging buffer is full with strange messages such as “readreadread.”

Conditions: This symptom is observed on a Cisco router with a 4-wire DSL WIC module that has the **logging buffered debugging** command enabled when an invalid message is accepted via the debug port TCP 1666.

Workaround: Configure buffer logging to the informational level or lower by entering the **logging buffered informational** command.

Access to the debug port can be blocked by deploying an interface access list that blocks access to the debug port TCP 1666 for traffic that is destined for any of the IP addresses of the router.

For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document: http://www.cisco.com/warp/public/707/tacl.html

For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document: http://www.cisco.com/warp/public/707/iacl.html

For information about using control plane policing to block access to the debug port, see the "Deploying Control Plane Policing White Paper:" http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper091 86a0080211f39.shtml

Note that the symptom does not impact other applications and services.

- 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.

- CSCsb19054

  Symptoms: When more than one PIM neighbor comes up and traffic passes through GRE+IPSec tunnels, a Cisco 7200 series that is configured with a hardware crypto engine pauses indefinitely because of a bus error.

  Conditions: This symptom is observed with multicast traffic.

  Workaround: There is no workaround.

- CSCsb20605

  Symptoms: A router that is configured for Intermediate Session Routing (ISR) stalls during the boot process.

  Conditions: This symptom is observed on a Cisco router that has an RTC and Certificate Server configuration in its startup configuration and that functions in either subordinate or RA mode.

  Workaround: Remove the Certificate Server configuration from the startup configuration.

- CSCsb22328

  Symptoms: You cannot differentiate the bandwidth reservation requirement for a G.722.1 codec. The bandwidth reservation for the G.722.1 codec is treated in the same way as for the G.711 codec.

  Conditions: This symptom is observed on a Cisco IP-to-IP (IPIPGW) gateway.

  Workaround: There is no workaround.

- CSCsb23054

  Symptoms: A handoff from a VXML document to a Tcl application does not work.

Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.4 or Release 12.4T when you use the <object> VXML construction to hand off the call leg to a Tcl application. The symptom is not platform-dependent.

Workaround: There is no workaround.

- CSCsb23143

  Symptoms: Calls to and from an H.323 platform via a gatekeeper-controlled H.225 trunk do not have a speech path in either direction.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series Communication Media Module (CMM) when a Media Termination Point (MTP), transcoding, or conferencing is involved and when the IP address of the Fast Ethernet interface that is used for the connection is not accessible.

  Workaround: Reset the CMM.

- CSCsb24007

  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

- CSCsb25054

  Symptoms: In an MPLS VPN environment, when you set up a Telnet session from a local CE or PE router to a remote CE router, the remote PE router crashes.

  Conditions: This symptom is observed on a Cisco 8800 series MGX RPM-XF that runs Cisco IOS Release 12.3(11)T3 or a later release, including Release 12.4, that functions as a remote PE router, and that has a multilink connection to the remote CE router. The remote CE router is a Cisco 7200 series that runs Cisco IOS Release 12.1 and that has the **bandwidth** command enabled on a virtual-template interface.

  Workaround: Upgrade the remote CE router to Cisco IOS Release 12.2 or a later release. If this is not an option and you must run Release 12.1 on the remote CE router, disable the **bandwidth** command.

- CSCsb25429

  Symptoms: A Cisco router that has a virtual-template interface that is configured for PPPoE may reload because of a software-forced crash.

  Conditions: This symptom is observed only when RADIUS AAA per-user attributes are used in active PPPoE sessions.

Workaround: There is no workaround.

- CSCsb26172

  Symptoms: When you configure “Timed Rollback,” a router reloads unexpectedly because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series.

  Workaround: There is no workaround. “Timed Rollback” is not yet supported.

- CSCsb27436

  Symptoms: A Cisco platform that is configured for SSG may reload unexpectedly because of a bus error, and generate a crashinfo file that shows the following error message:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  ```

  Conditions: This symptom is observed when the **no host overlap** command is enabled and when users connect and disconnect.

  Workaround: Remove the **no host overlap** command. If this is not an option, there is no workaround.

- CSCsb28315

  Symptoms: The “tunnel protection malloc” process may cause a memory leak in the Crypto IKMP process.

  Conditions: This symptom is observed on a Cisco platform that runs a crypto image and that functions as a spoke when the interface that connects to the hub flaps and receives a new IP address after the flap.

  Workaround: There is no workaround.

- CSCsb28691

  Symptoms: A Cisco gateway GPRS support node (GGSN) that functions under stress may reload unexpectedly.

  Conditions: This symptom is observed when the call rate is high (200 calls per second), when there are two DHCP servers that respond very slowly, and when the GGSN is configured for session redundancy.

  Workaround: There is no workaround.

- CSCsb28818

  Symptoms: A few permanent virtual circuits (PVCs) enter a stuck state, causing OutPktDrops, and all Layer 3 protocols through the affected subinterfaces are down.

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-PR and can occur even without any change in the configuration.

  Workaround: Remove and re-apply the PVC statement and the switch connections.

- CSCsb29096

  Symptoms: A router may crash when an OSPF adjacency is established across an ISDN backup link. The router reports a bus error and generates a corrupted PC address.

  Conditions: This symptom is observed on a Cisco router that functions in SRST fallback mode and that is configured for Multicast Music on Hold when the following sequence of events occurs:

  – A Frame Relay PVC fails on the router.
  – ISDN comes up as a backup connection.
  – The OSPF adjacency is re-established.

  Workaround: There is no workaround.

- CSCsb31564

  Symptoms: A ping does not pass through an FRF8 circuit that is configured for service internetworking.

  Conditions: This symptom is observed on a Cisco IAD2430 that runs Cisco IOS interim Release 12.4(2.12a).

  Workaround: There is no workaround.

- CSCsb33129

  Symptoms: A router may reload unexpectedly when the SSG queue for RADIUS requests that are in the waiting state becomes too large.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(14)T1 or Release 12.4(1a) and that is configured for SSG. When there is a large number of RADIUS requests or a connectivity problem between SSG and the RADIUS server, the SSG queue for RADIUS requests that are in the waiting state may become too large.

  Workaround: There is no workaround.

- CSCsb34344

  Symptoms: A Fast Ethernet (FE) interface on a Cisco AS5400 may reset unexpectedly.

  Conditions: This symptom is observed when you attempt to program the FE controller for multicast or broadcast traffic such as OSPF, EIGRP, RIP, or PIM.

  Workaround: There is no workaround.

- CSCsb34361

  Symptoms: The queue size value of a VC CoS is not properly updated for a congestion management algorithm that is based on Early Packet Discard (EPD).

  Conditions: This symptom is observed on a Cisco RPM-XF that is configured as XFL and that has SAR-based QoS enabled when the congestion management algorithm is changed from Weighted Random Early Detection (WRED) to EPD.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected subinterface or reprogram the affected CoSQ.

- CSCsb37645

  Symptoms: A router may crash during a basic H.323 call with carrier ID routing.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(3.3).

  Workaround: There is no workaround.

- CSCsb39765

  Symptoms A GGSN fails to establish a TCP path with a charging gateway.

  Conditions: This symptom is observed when the path protocol is TCP.

  Workaround: There is no workaround.

- CSCsb40055

  Symptoms: A service name is absent from a service authorization request packet that is sent by an SSG to a prepaid server.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG.

  Workaround: There is no workaround.

- CSCsb40194

  Symptoms: A Cisco 7301 that is configured for SSG may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when a user with an active session logs in again. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsb42176

  Symptoms: A Cisco 7200 series may pause indefinitely when a neighbor reloads.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-POS-2OC3 port adapter.

  Workaround: There is no workaround.

- CSCsb42362

  Symptoms: Egress packets are dropped from traffic flows that are configured for compression.

  Conditions: This symptom is observed on a Cisco 2851, Cisco 3825, and Cisco 3845 that have an onboard encryption engine that accelerates IPSec flows with IP compression with the Lempel-Ziv-Stac (LZS) algorithm (comp-lzs).

  Workaround: Disable the hardware encryption engine, disable the compression for the IPSec flow, or disable both.

- CSCsb42374

  Symptoms: There are two symptoms:

  1. When a policy is attached to the incoming interface, an aggregate control- plane policing policy will not classify traffic correctly.
  2. When a control-plane policing policy is attached to the aggregate path, a similar policy attached to the host, transit or cef-exception paths will not classify traffic correctly.

  Conditions: These symptoms have been observed on a Cisco platform that runs Cisco IOS Release 12.3T or Release 12.4.

  Workaround: Any existing interface policy would have to be removed for the aggregate control-plane policing policy to work. Any existing aggregate policing policy will have to removed for the host/cef-exception/transit path control-plane policing policy to work.

- CSCsb42859

  Symptoms: A router may reload unexpectedly when the stack for VTSP runs low in memory.

  Conditions: This symptom is observed on a Cisco router that functions as a voice gateway.

  Workaround: There is no workaround.

- CSCsb43117

  Symptoms: Media negotiation fails for SIP calls and the terminating gateway replies with a “488” message to an Invite message.

  Conditions: This symptom is observed on a Cisco platform when the terminating gateway is configured with the G279B (annex B) codec and when the Session Description Protocol (SDP) for the incoming Invite message does not have any FMTP attribute line, which means that the default value, that is, the G279B (annex B) codec, is used.

  Workaround: There is no workaround.

- CSCsb46264

  Symptoms: When a dialer interface is configured as an endpoint for a IPSec+GRE tunnel, tracebacks with bad refcount may be generated.

  Conditions: This symptom is observed on a Cisco 837 when router-generated packets such as routing updates are being switched.

  Workaround: There is no workaround.

- CSCsb47257

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

  Conditions: This symptom is observed on a Cisco router that is configured for IPSec.

  Workaround: There is no workaround.

- CSCsb47438

  Symptoms: A CoSQ creation fails while switching between Weighted Random Early Detection (WRED) and Early Packet Discard (EPD).

  Conditions: This symptom is observed on a Cisco RPM-XF that is configured as XFL when "max 8" CoS queues are configured under a VC tunnel and when traffic is queued in a CoS queue. When you attempt to switch the CoS queue congestion management policy, the SAR queue creation fails.

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

- CSCsb50143

  Symptoms: You cannot create a maximum session number for a DSPfarm profile conference.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T or Release 12.4(1a) when time slot 1 through 24 of the PRI group are configured before you attempt to create a maximum session number. The symptom occurs on an NM-HDV2 that has a PVDM2-64 installed.

  Workaround: First configure a maximum session number for the DSPfarm profile conference, then configure time slot 1 through 24 of the PRI group.

  Do not reload the gateway or enter the **shutdown** command for the DSPfarm profile after everything is properly configured because otherwise the PRI group would grasp all the DSP resources again.

- CSCsb50995

  Symptoms: The Switch Processor (SP) of a Cisco Catalyst 6500 series or Cisco 7600 series may run out of memory with 15,000 VPLS VCs (that is, with 512 VFIs and 30 LDP neighbors).

  Conditions: This symptom is observed when all LDP sessions are flapped many times with a pause of approximately 10 seconds between each flap.

  Workaround: There is no workaround.

- CSCsb51663

  Symptoms: The SNMP process hangs while a QoS MIB object is queried.

  Conditions: This symptom is observed when the execution of a QoS **show** command is in the "More" state while the QoS MIB object is queried. The SNMP process resumes when the **show** command is finished. Depending on the SNMP configuration, different symptoms may occur while the SNMP process is waiting for the QoS **show** command to finish.

  Workaround: There is no workaround.

- CSCsb52317

  Symptoms: A Cisco 1700 series that is configured with a voice image may crash.

  Conditions: This symptom is observed when you boot a Cisco 1700 series that runs Cisco IOS interim Release 12.4(3.6) or a later interim release or Release 12.4(3.6)T or a later interim release.

  Workaround: There is no workaround.

- CSCsb52988

  Symptoms: When a user of a local IP phone calls a CUE AA application to reach another user (or the voice mail) of an IP phone via a "dial-by-extn" scenario, tones are not played properly and the users cannot talk to each other.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that supports the Distributed Stream Media Processor (DSMP). Note that the symptom does not occur when a user of a remote IP phone calls a CUE AA application to reach a user of another local or remote IP phone.

  Workaround: There is no workaround.

- CSCsb54084

  Symptoms: Entering a DTMF input triggers a "noinput" event instead of a recognition or "nomatch" event. This situation occurs regardless of when the DTMF key is pressed.

  Conditions: This symptom is observed on a Cisco platform that functions as a CVP VXML Server.

  Workaround: There is no workaround.

- CSCsb54726

  Symptoms: A call is incorrectly disconnected when the hold button of an IP phone is pressed.

  Conditions: This symptom is observed in a scenario in which an IP phone is connected to a Cisco CallManager that is connected to an IPIPGW that, in turn, is connected to another Cisco CallManager.

  Workaround: There is no workaround.

- CSCsb56867

  Symptoms: A Cisco IOS VoIP gateway may reload unexpectedly.

  Conditions: This symptom is observed when an attempt is made to poll some SNMP information from the gateway while the gateway processes voice and fax calls.

  Workaround: Disable SNMP. If this is not an option, there is no workaround.

- CSCsb57390

  Symptoms: When you enter the **dtmf-relay rtp-nte** command, all **voice-class sip** commands are unexpectedly removed from the configuration.

  Conditions: This symptom is observed when **voice-class sip** commands are enabled on a VoIP dial peer and when you enter the **dtmf-relay rtp-nte** command on the VoIP dial peer.

  Workaround: There is no workaround.

- CSCsb58117

  Symptoms: A GE interface that functions in promiscuous mode cannot receive multicast traffic, causing a difficulty with HSRP or with a routing protocol such as OSPF or EIGRP because the GE interface cannot receive multicast hello packets.

  Conditions: This symptom is observed when the GE interface has eight or more subinterfaces and when all subinterfaces are configured for HSRP.

Workaround: Enable PIM on one of the subinterfaces.

- CSCsb59555

  Symptoms: An Engine 3 or Engine 4+ line card may be stuck in the "request reload" state and CEF may be disabled on the line card, although the CEF table is up, as is shown in the output of the **show cef linecard** command:

```
Slot      MsgSent    XDRSent  Window   LowQ   MedQ  HighQ Flags
 1            8558     719895    4966      0      0      0 up
 2            8560     718293    4966      0      0      0 up
 3            8609     722867    4965      0      0      0 up
 4            8584     721311    4965      0      0      0 up
 5            8597     724307    4965      0      0      0 up
 9            8586     722060    4966      0      0      0 up
 10           8579     720566    4966      0      0      0 up
 11           8566     719086    4966      0      0      0 up
 12           8606     725072    4966      0      0      0 up
 13           8597     723572    4966      0      0      0 up
*7               1          3      24      0      0      0 disabled, rrp hold
 0            4058     359354    4966      0      0      0 up
VRF Default, version 5032, 5024 routes
 Slot   Version    CEF-XDR    I/Fs State    Flags
 1         5032       5016      67 Active   sync, table-up
 2         5032       5016       5 Active   sync, table-up
 3         5032       5016      20 Active   sync, table-up
 4         5032       5016       5 Active   sync, table-up
 5         5032       5016       5 Active   sync, table-up
 9         5032       5016       4 Active   sync, table-up
 10        5032       5016       4 Active   sync, table-up
 11        5032       5016      20 Active   sync, table-up
 12        5032       5016       4 Active   sync, table-up
 13        5032       5016       8 Active   sync, table-up
*7            0          0       4 Active   table-disabled
 0            0          0       5 Active   request reload, table-up
```

  Conditions: This symptom is observed on a Cisco 12000 series after an RPR+ switchover has occurred. However, the symptom is platform-independent and may also occur on another platform that is configured for CEF when an RPR+ switchover has occurred.

  Workaround: Enter the **clear cef linecard** command for the affected line card.

- CSCsb60049

  Symptoms: When you reload a Cisco VoIP gateway that is configured as a CCM manager, the gateway pauses indefinitely.

  Conditions: This symptom is observed when the Cisco VoIP gateway has the **ccm-manager mgcp** global configuration command configured.

  When you enter the **reload** command via a vty EXEC session (that is, via a Telnet session), the console is accessible but the router is still stuck in a semi-functional state in which some processes are running and others are not. Attempting to reload the router again from the console does not succeed, and the router generates "%Reload in progress" message.

Workaround: To resolve the symptom, either power-cycle the gateway or, if the break mode is enabled on the console, reset the gateway from the ROMmon mode by sending a break to the console.

To prevent the symptom from occurring, remove the **no ccm-manager mgcp** global configuration from the configuration before you reload the router.

- CSCsb60714

  Symptoms: The **mpls ldp router-id** *interface* **force** command is not accepted by the router.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series when the interface in the *interface* argument of the **mpls ldp router-id** *interface* **force** command is not yet configured. The symptom may also affect other platforms.

  Workaround: First, configure the interface that you intend to use for the LDP router ID. Then, enter the **mpls ldp router-id** *interface* **force** command.

- CSCsb63090

  Symptoms: The Embedded Event Manager TCL **action_switch** command expects arguments when it should not receive any arguments.

  Conditions: This symptom is observed when an Embedded Event Manager TCL policy is configured to use the **action_switch** command.

  Workaround: Configure the **action_switch primary 1** command in the Embedded Event Manger TCL policy at the location where the **action_switch** command is needed.

- CSCsb64721

  Symptoms: A spurious access is generated on a Cisco 7500 series and a virtual-access interface does not come up but remains in the up/down state.

  Conditions: These symptoms are observed on a Cisco 7500 series that is configured for dLFIoFR when the MTU size is changed on the physical interface.

  Workaround: There is no workaround.

- CSCsb65056

  Symptoms: A PPP connection may remain active after the idle-timer zeroes out. This situation may affect other services that rely on the termination of the PPP connection. Also, an incorrect redirection may occur.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG when the host object is disconnected but the PPP connection remains active.

  Workaround: There is no workaround.

  Further Problem Description: After the host idle-timeout/user idle-timeout in the output of the related virtual access interface, you can troubleshoot the situation through the **debug ssg events** command.

- CSCsb65867

  Symptoms: Intermittent one-way voice occurs between an IP phone and an NM-HDV2 network module.

  Conditions: This symptom is observed on a Cisco platform that functions as an MGCP gateway and that is configured with an NM-HDV2 network module.

  Workaround: There is no workaround.

- CSCsb69726

  Symptoms: A Cisco IOS Client could not understand the back server list if it has more than one back server pushed by the Cisco VPN 3000 Concentrator.

  Conditions: This symptom has been observed on all releases supporting the back server feature and is applicable only for a Cisco VPN 3000 Concentrator with a Cisco IOS Client.

  Workaround: Do not add more than one backup server to the client group configuration of the Cisco VPN 3000 Concentrator.

  Further Problem Description: As per the Unity Client protocol during the mode configuration reply, the back server list pushed by the concentrator can be delimited by " ,\r\n|". Since the Cisco IOS Client does not understand the "" space delimiter sent by the Cisco VPN 3000 Concentrator, the Cisco IOS Client misunderstands the entire back up server list as a single backup server.

- CSCsb72269

  Symptoms: Unity Express Message Waiting Indication (MWI) is not turned on when it should be turned on.

  Conditions: This symptom is observed when IVR is enabled under the **telephony-service** and **ephone-dn** commands.

  Workaround: There is no workaround.

- CSCsb74409

  Symptoms: A router may keep the vty lines busy after finishing a Telnet/Secure Shell (SSH) session from a client. When all vty lines are busy, no more Telnet/SSH sessions to the router are possible.

  Conditions: This symptom is observed on a Cisco router that is configured to allow SSH sessions to other devices.

  Workaround: Clear the SSH sessions that were initiated from the router to other devices.

- CSCsb77335

  Symptoms: A router may crash when you enter the **show memory fragment detail** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCsb80536

  Symptoms: A Cisco 3640 router may fail to boot with an image of Cisco IOS Release 12.3 and may enter the ROMmon during the boot process.

  Conditions: This symptom is observed only on a Cisco 3640.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2T. The fix for this caveat is also integrated in Release 12.4 and Release 12.4T.

  Further Problem Description: If the router boots an image successfully once, then it is safe to assume that the symptom will not occur on the router.

- CSCsb84354

  Symptoms: A memory leak occurs when a midcall INVITE fails media negotiation for an incoming "200". Eventually, this leak causes memory fragmentation and causes the platform to reload.

Conditions: This symptom is observed on a Cisco AS5850 gateway that runs Cisco IOS Release 12.3(14)T3 but may also occur in Release 12.4 and Release 12.4T. The symptom occurs when the gateway sends a "a=T38MaxBitRate:7200" and when the other side responds incorrectly with a "a=T38MaxBitRate:14400". The gateway functions properly by failing media negotiation but the incorrect SDP data is released, causing the leak.

Workaround: There is no workaround.

- CSCsb90264

  Symptoms: Cisco AS5400 and AS5350 T1 CAS calls fail with "no users answer," and a traceback is seen at "vtsp_tsp_call_setup_ind," along with the following error:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
  ```

  Conditions: This problem is seen when making CAS calls in Cisco AS5400 and AS5350 platforms.

  Workaround: There is no workaround.

- CSCsb90439

  Symptoms: FXS ports of a Communication Media Module (CMM) or are not registered in MGCP mode.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run Cisco IOS Release 12.4. The symptom could also occur in Release 12.4T.

  Workaround: There is no workaround. Note that the symptom does not occur in H.323 mode.

- CSCsb92374

  Symptoms: When you enter the **no rd** command, the subsequent configuration or unconfiguration of the **rd** command for the VRF fails.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release and 12.4 (no other releases are affected) when the **router bgp** and **address-family vpnv4** commands are not enabled and when the fix for caveat CSCeh12594 is integrated in the release. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh12594. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Enter the **router bgp** command followed by the **address-family vpnv4** command.

  Further Problem Description: The symptom occurs because a flag is set when you enter the **no rd** command for a VRF. Resetting the flag is essential to complete the process and occurs in a service routine that is registered only if the VPNv4 address family is configured for BGP. The fix for this caveat checks whether or not the VPNv4 address family is configured for BGP, and does not reset the flag if the VPNv4 address family is not configured for BGP.

- CSCsb92920

  Symptoms: A router that is configured for IPHC may crash when you remove a service policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4 or 12.4T but may also occur on other platforms. The symptom occurs when you enter the following sequence of commands:

  ```
  frame-relay switching
  class-map match-all voip
   match protocol ip
  policy-map p1
   class voip
    compress header ip
  ```

```
interface Serial6/0
 encapsulation frame-relay
 service-policy output p1
no shutdown
interface Serial6/0
 shutdown
 no  service-policy output p1
 no  encapsulation frame-relay
```

Workaround: There is no workaround.

- CSCsb94575

  Symptoms: A Cisco 2600XM series may crash because of a SegV exception.

  Conditions: This symptom is observed on a Cisco 2600XM series that runs Cisco IOS Release 12.4(3) when you enter the **show ephone login** command.

  Workaround: There is no workaround.

- CSCsb96968

  Symptoms: SSG TCP redirection does not occur.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG and occurs for prepaid users.

  Workaround: There is no workaround.

- CSCsb98254

  Symptoms: A router may fail when you reload a Gigabit Ethernet (GE) line card or port adapter that has link-bundling enabled.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S and that is configured for MPLS. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- CSCsb99256

  Symptoms: A Cisco 7500 series may pause indefinitely during the boot process right after the image is successfully decompressed.

  Conditions: This symptom is observed on a Cisco 7500 series that is booted with Cisco IOS interim Release 12.4(4.8). The symptom could also occur in Release 12.4T.

  Workaround: There is no workaround.

- CSCsb99906

  Symptoms: A host name domain lookup takes too long, the following error message is generated, and the CP-to-CP session is terminated:

  ```
  %SNASW-4-CPUUsage: SNASw process, type 0x603 ran for 18000 ms processing IPS of type
  0x5103, address 0x65D1DC30
  ```

  Conditions: This symptom is observed on a Cisco platform that functions as a SNASwitch and that runs Cisco IOS Release 12.4(1a).

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3.

- CSCsc02825

  Symptoms: In Cisco IOS software that is running the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the router could reload while trying to access a bad virtual address.

  Conditions: This symptom may be observed when LDP is being used. It will not be observed with TDP. It may happen when LDP receives a protocol message larger than 512 bytes right after receiving several Label Mapping messages smaller than 25 bytes. This problem is likely to be accompanied by the presence of one of the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xD0D0D0D
  ```

  The above error message may be preceded by one of the following four error messages:

  ```
  %ALIGN-1-FATAL: Corrupted program counter 19:45:07 CET Mon Sep 26 2005
      pc=0xD0D0D0D, ra=0x61164128, sp=0x64879B98
  %TDP-3-BAD_PIE: peer x.x.x.x; unknown pie type 0x11E
  %TDP-3-UNEXPECTED_PIE: peer x.x.x.x unexpected pie type 0x0
  %TDP-3-PTCLREAD: peer x.xx.x0, read failure
  ```

  This problem may be seen in releases that include the fix for CSCeg74562 but do not have the fix associated with this defect.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCeh35980

  Symptoms: A router may reload in a TCP function.

  Conditions: This symptom is observed in a complex scenario with a large number of BGP peers when neighbors are shut down and brought up again.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCee85138

  Symptoms: A SegV exception crash may occur on a Cisco router that is configured for voice calls.

  Conditions: This symptom is observed on a Cisco 2600 series that runs Cisco IOS Release 12.3(6a) or Release 12.3(9) but may not be platform-dependent.

  Workaround: There is no workaround.

- CSCeg20283

  Symptoms: E1R2 SS7 calls fail to come up when more than one call is made with the following ISDN error:

  ```
  ISDN Se1/6:15 SC **ERROR**: call_connect: call_id not found, rejecting call
  ISDN **ERROR**: Module-CCPRI Function-CCPCC_CallConnected Error-Unknown event
  received in message from L3 or Host: 4F
  ```

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(11)T.

  Workaround: There is no workaround.

- CSCeg62022

  Symptoms: A DSL stops responding to ISDN calls (no response to SETUP messages). An "L3_GetUser_NLCB returned NULL" Q931 debug message may generated for each failed call.

  Conditions: This symptom is observed intermittently on a Cisco router.

  Workaround: There is no workaround.

- CSCeh49616

  Symptoms: Incoming MPLS packets with IETF Frame Relay encapsulation are process-switched.

  Conditions: This symptom is observed only on a Cisco 7200 series.

  Workaround: Do not configure IETF Frame Relay encapsulation. Rather, configure Cisco Frame Relay encapsulation.

- CSCeh71921

  Symptoms: When the **radius-server retransmit 1** command is enabled on a NAS, the number of retransmit counts for a callback call transaction with a Microsoft Internet Access Service (IAS) server is below the expected value.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release 12.4(1.6).

  Workaround: There is no workaround.

- CSCei11919

  Symptoms: A dialed circuit that carries a PPP connection over a tunnel between an LNS and a LAC is not dropped when the tunnel is reset.

  Conditions: This symptom is observed when you enter the **clear vpdn all** command, when the LNS reloads, when the IP link between the LSN and LAC is disrupted, or when any other event occurs that causes the tunnel to be reset.

  Workaround: There is no workaround.

- CSCei13743

  Symptoms: An outgoing Basic Rate Interface (BRI) call fails to activate the layer 1.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that includes the fix for caveat CSCsa66756. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa66756. 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.

- CSCei16649

  Symptoms: The output of the **show pppoe session** or **show vpdn session** command does not show PPPoEoA session details.

  Conditions: This symptom is observed for a point-to-point ATM interface.

  Workaround: There is no workaround.

- CSCei19158

  Symptoms: Alignment errors may be generated when you remove a Multi-VC configuration. The output of the **show align** may look as follows:

```
Address  Count  Traceback
      50      1  0x60DA1C20 0x60DA51AC 0x60DACED0 0x60DADCBC
```

```
            0x60DA5BBC
6C      1   0x60DA1C28 0x60DA51AC 0x60DACED0 0x60DADCBC
            0x60DA5BBC
50      1   0x60DA1C30 0x60DA51AC 0x60DACED0 0x60DADCBC
            0x60DA5BBC
24      1   0x60DA1C44 0x60DA51AC 0x60DACED0 0x60DADCBC
            0x60DA5BBC
28      1   0x60DA1C4C 0x60DA51AC 0x60DACED0 0x60DADCBC
            0x60DA5BBC
```

Conditions: This symptom occurs at a rate of about one in twenty cases on a Cisco 10000 series that is configured with many Multi-VC MLPoATM multilink bundles. However, the symptom is platform-independent.

Workaround: There is no workaround.

- CSCei19546

  Symptoms: The output of the **show ppp mppe** {**serial** | **virtual-access**} [*number*] command does not show the current connection information.

  Conditions: This symptom is when you check the MPPE negotiation status.

  Workaround: There is no workaround.

- CSCei20503

  Symptoms: A router reloads unexpectedly when you perform a netboot procedure.

  Conditions: This symptom is observed on a Cisco router that is configured with a dialer profile when you attempt to perform a netboot procedure via a boothelper image.

  Workaround: Unconfigure the dialer profile before you perform a netboot procedure.

  Alternate Workaround: Boot the router from a Cisco IOS software image on a disk that is installed in a slot of the router.

- CSCei21549

  Symptoms: A Cisco 5850 reloads when an RLM group is unconfigured.

  Conditions: This symptom is observed when you enter the **no isdn rlm-group** *number* command and when there are more than 31 NFAS members in the same NFAS group.

  Workaround: Shut the primary interface, remove the NFAS members of the same NFAS group, and unconfigure the RLM group.

- CSCei88594

  Symptoms: A router that is configured for Frame Relay crashes and generates the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x68, pc=0x621D6C50 ,
  ra=0x621D8214 , sp=0x649990A8
  ```

  Conditions: This symptom is observed on a Cisco router that has Frame Relay end-to-end fragmentation configured on an interface and hardware compression on a PVC.

  Workaround: Configure map-class fragmentation with Frame Relay traffic-shaping instead of interface level fragmentation.

- CSCej08045

  Symptoms: A router reloads unexpectedly when you enter the **debug vpdn packet** command.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(3.9)T1 when the **ip cef** command is enabled. The symptom may also affect other platforms and may also occur in Release 12.4.

Workaround: Do not enter the **debug vpdn packet** command.

First Alternate Workaround: Disable CEF by entering the **no ip cef** command before you enter the **debug vpdn packet** command. When the debug output is generated, re-enable CEF by entering the **ip cef** command.

Second Alternate Workaround: When traffic has started to flow, enter the **show vpdn** command before you enter the **debug vpdn packet** command.

- CSCej45061

  Symptoms: Attempts to remove a PRI group fail.

  Conditions: This symptom is observed when an NFAS group has group number 0 and when you attempt to remove a FAS PRI group.

  Workaround: Shut down the NFAS group before you remove the FAS PRI group.

- CSCin92814

  Symptoms: A router crashes when you enter the **no ip vrf** *vrf-name* global configuration command.

  Conditions: This symptom is observed only when you remove the VRF configuration immediately after removing VRF forwarding from an interface.

  Workaround: Wait for 60 seconds between removing VRF forwarding from the interface and removing the VRF configuration.

- CSCsa42221

  Symptoms: A call reference flag is missing from a TBCT request message to a third-party vendor ISDN switch.

  Conditions: This symptom is observed on a Cisco AS5400 but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCsa55747

  Symptoms: The RADIUS L2TP-specific disconnect code value for the Ascend-Disconnect-Cause RADIUS attribute (195) is incorrectly generated as 607 instead of 605.

  Conditions: This symptom is observed when an L2TP tunnel setup failure occurs between a LAC and an LNS.

  Workaround: There is no workaround.

- CSCsa73159

  Symptoms: No final billing record is made for a call.

  Conditions: This symptom is observed when a call is made using a Two B-Channel Transfer (TBCT) TCL script in the following scenario:

  - The Telco switch signals the TBCT call with a special FACILITY message.
  - A call leg is created between point A and point B, and another call leg is created between point C and point D.
  - TBCT connects point A to point D to release the TDM resources.
  - A billing start record is made for each call leg.
  - When the final call between point A and point D is released and a NOTIFY message is received, no final billing record is made for this call.

Workaround: There is no workaround.

- CSCsb26163

  Symptoms: Tracebacks are generated in the “isdn_carrier_timeout” function during a dialout test.

  Conditions: This symptom is observed only when the **dialer order round-robin** command is enabled.

  Workaround: Try a different dialer order such as last successful or sequential to prevent the tracebacks from being generated.

- CSCsb45201

  Symptoms: A router crashes during RBP data transfer in the direction from X.25 to RBP.

  Conditions: This symptom is observed only when RBP receives an X.25 data packet that is larger than the configured RBP record size.

  Workaround: On the RBP map, configure the RBP record size to be larger than the maximum X.25 packet size.

- CSCsb58447

  Symptoms: In a VPDN callback configuration, a callback call is successfully initiated and connected. However, when IPCP is successfully negotiated, the LNS receives an LCP CONFREQ message, causing the established PPP session to be disconnected and LCP to renegotiate again. This situation repeats itself continuously and may cause sporadic IP connectivity. Eventually, the call is cleared completely because the tunnel is disconnected by the LAC.

  The output of the **debug ppp negotiation** command on the LAC shows that the LAC never finishes the PPP LCP negotiation with the client during the callback call. This situation causes the LAC to disconnect the tunnel.

  Conditions: This symptom is observed on a Cisco 3660. However, the symptom is platform-independent.

  Workaround: Enter the **no ppp lcp fast-start** command on the relevant asynchronous interfaces on the LAC.

- CSCsb83459

  Symptoms: A router may reload when many PPPoE sessions are being initiated while memory availability is low or when many PPPoE sessions are being initiated and terminated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(12.5) or a later release, interim Release 12.3(12.4)T or a later release, or any release of Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(3j)

Cisco IOS Release 12.4(3j) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3j) but may be open in previous Cisco IOS releases.

- CSCsl68368

  Symptoms: The image c2801-advipservicesk9-mz.124-3i.bin fails to load using the **tftpdnld-r** command with the following error message:

  ```
  *** TLB (Load/Fetch) Exception ***
  Access address = 0x0
  ```

```
PC = 0x0, Cause = 0x8, Status Reg = 0x34410002
```

Conditions: This symptom occurs when loading c2801-advipservicesk9-mz.124- 3i.bin.
Workaround: Do not load c2801-advipservicesk9-mz.124-3i.bin.

Further Problem Description: c2801-advipservicesk9-mz.124-3i.bin is a bad built image.

Resolved Caveats—Cisco IOS Release 12.4(3i)

Cisco IOS Release 12.4(3i) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3i) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsk70446

  Cisco IOS emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

  A traceback appears after the error message. This traceback is encountered with long URLs.

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

Miscellaneous

- CSCsg91306

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsh74975

  Symptoms: A router may reload or a leak memory may occur when UDP malformed packets are sent to port 2517.

  Conditions: This symptom is observed on a Cisco router that functions as a VoIP dial peer and that is configured for H.323.

  Workaround: There is no workaround.

- CSCsj66692

  Symptoms: Data corruption copy error tracebacks are seen on the console or output from the **show logging** command:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,  -PC= 0x41224EFC,
  ```

```
-Traceback= 0x4153A7D0 0x4155BA0C 0x4157FAF0 0x41224EFC 0x41DDC0A8 0x41DDC198
0x41DC6D84 0x41DF3B0C 0x41DC506C 0x41DCE5A4 0x41D91AF8 0x41D90F88 0x41D9BEFC
0x41D9C0C0 0x41DAEA68
```

Conditions: Refer to CSCsj44081 for more information.

Workaround: There is no workaround.

- CSCsj95947

  Symptoms: The following message is seen on the router:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
-PC= 0x8005EC50,
-Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50 0x800651E4 0x800652A8
0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0 0x809E42D4 0x80A0854C 0x800DB8C0
0x800DEE48
```

  Conditions: The conditions under which this symptom occurs are not known at this time.

  Workaround: There is no workaround.

- CSCsk73104

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml

TCP/IP Host-Mode Services

- CSCsh04686

  Symptoms: With X25 over TCP (XOT) enabled on a router or catalyst switch, malformed traffic sent to TCP port 1998 will cause the device to reload. This was first observed in Cisco IOS Release 12.2(31)SB2.

  Conditions: Must have “x25 routing” enabled on the device.

  Workarounds: Use IPSEC or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is only accepted from trusted tunnel endpoints.

Wide-Area Networking

- CSCeh64479

  Symptoms: A router reloads unexpectedly when an apparent Layer Two Forwarding (L2F) packet is received.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Virtual Private Dialup Network (VPDN). However, the symptom is not platform-specific.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(3h)

Cisco IOS Release 12.4(3h) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3h) but may be open in previous Cisco IOS releases.

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.

- 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

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

Miscellaneous

- 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.

- 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

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  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.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM) CSCsi97695

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

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

  Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle. shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.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.

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t
  ip ssh version 1
  end
  ```

  Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

  ```
  10.1.1.0/24 is a trusted network that
  is permitted access to the router, all
  other access is denied

  access-list 99 permit 10.1.1.0 0.0.0.255
  access-list 99 deny any

  line vty 0 4
  ```

```
access-class 99 in
end
```

Further Problem Description: For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6350_TSD_Products_Configuration_Guide_Chapter.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.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

- CSCsg96319

  Symptoms: When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:***number ip-address* command.

  Conditions: This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_rev_ssh_enhanmt_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  Workaround: Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

- CSCsh58082

  Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

  There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

  Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi67763

  The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

  http://www.kb.cert.org/vuls/id/739224

  By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

  Cisco response is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml

- CSCsi84017

  Symptoms: When you reload a Cisco 2600 series, the router may hang.

Conditions: This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

Workaround: There is no workaround.

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 12.4(3g)

Cisco IOS Release 12.4(3g) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3g) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCej30903

  Symptoms: A router allows logging into the root (or any other configured) view without prompting for a password.

  Conditions: This symptom is observed when no method list is configured for login service.

  Workaround: Configure a method list for the login service.

- CSCsa43465

  Symptom: Users under specified conditions may be able to access privilege level 15 without entering a password.

  Conditions: In Cisco IOS Release 12.3(7)T and later, which support Role-Based CLI Access, the use of the **none** keyword in the default login method list may allow users to enter root view mode (privilege level 15) without entering a password.

  Example, if the customer configures:

  aaa authentication login default group tacacs+ none

  If the TACACS+ server is down, users are allowed to enter non-privileged mode. However, they can also enable into root view access through the **enable view** command without having to enter a password.

  Workaround: The resolution of the DDTS puts authentication of the **enable view** command to the default enable method list.

Prior to software upgrade, a workaround is to ensure that the method **none** is not in the default login methods list.

- 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.

Miscellaneous

- CSCee72997

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCin96617

  Symptoms: A router that has SSG enabled may refuse new incoming connections (either Telnet, PPP, or any type of AAA connection).

  Conditions: This symptom is observed when a very large amount of memory is held by SSG as a result of multiple IPCP negotiations for a PPP session.

  Workaround: There is no workaround.

- CSCin99565

  Symptoms: A router that is configured for SSG may reload unexpectedly.

  Conditions: This symptom is observed when both the Transparent Auto-Logon (TAL) and Port-Bundle Host-Key (PBHK) SSG features are enabled and when it takes a long time before the AAA server responds.

  Workaround: There is no workaround.

- CSCsb54726

  Symptoms: A call is incorrectly disconnected when the hold button of an IP phone is pressed.

  Conditions: This symptom is observed in a scenario in which an IP phone is connected to a Cisco CallManager that is connected to an IPIPGW that, in turn, is connected to another Cisco CallManager.

  Workaround: There is no workaround.

- CSCsb65867

  Symptoms: Intermittent voice quality including one-way audio towards the PSTN side of a VoIP call.

Conditions: This can occur when excessive jitter is present on the IP network side impacting the incoming RTP stream to the IOS VoIP gateway. This is present only when using MGCP controlled voice ports and Cisco IOS 12.3.14T and higher.

The issue stems from the jitter buffer playout mode for that call being set to a fixed mode of 65msec versus adaptive mode.

The typical symptom would be that voice quality may degrade for calls where excessive jitter is present in the RTP stream.

This issue can be confirmed by checking the output of the exec command **show call act voice** for an active call experiencing voice quality problems. This problem can be seen when the late packets count is increasing but the PlayoutDelayCurrent as well as the PlayoutDelayMax is fixed at 65msec. See snippet of this command output below:

```
-----
RxLatePak=23
RxEarlyPak=0
PlayDelayCurrent=65
PlayDelayMin=65
PlayDelayMax=65
----
```

Workaround: Use H323 instead of MGCP or use Cisco IOS Release 12.3(11)T.

- CSCsd35389

  Symptoms: When a Cisco Unified CallManager Express (Cisco Unified CME) registers with a gatekeeper, all the ephone-dns are automatically registered. When an ephone-dn is deleted, it does not unregister with the gatekeeper. If you enter the **no gateway** command followed by the **gateway** command on the CME router to force it to unregister then reregister, the deleted ephone-dn will show up again.

  Conditions: This symptom is observed on a Cisco 3800 series router.

  Workaround: To permanently remove the ephone-dn reload the CME/gateway or enter the **shut** command followed by the **no shut** command on the gatekeeper.

- CSCsd76444

  Symptoms: A Cisco router may reload unexpectedly with a “Signal 0” without a stack trace in the crash info file.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE and that is configured for SSG. However, the symptom is platform-independent and may occur on any router that is configured for SSG.

  Workaround: There is no workaround.

- CSCse03855

  Symptoms: An IP phone display remains stuck at “Enter Number” for the duration of an outgoing call to the PSTN.

  Conditions: This symptom is observed when the IP phone runs CME version 3.3 and is connected to a BRI ISDN interface on a Cisco router that runs Cisco IOS Release 12.4. When you enable the **debug isdn q931** command, the following message is displayed in response to an outgoing setup message:

  ```
  ISDN BR0/2/0 Q931: RX <- SETUP_ACK pd = 8  callref = 0x83
  Channel ID i = 0x89
  Progress Ind i = 0x8288 - In-band info or appropriate now available
  ```

Workaround: Prevent the Telco from sending the following information in the setup_ack message:

```
Progress Ind i = 0x8288 - In-band" information or appropriate now available
```

Note that the symptom does not occur in Cisco IOS Release 12.3(11)T10 and with CME version 3.2.

- CSCse05642

  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

- CSCse42141

  Symptoms: T38 fax calls fail when they come inbound through DID Analog ports. In the debug h245 asn1, there is no OLCAck sent back towards the fax server.

  Conditions: This symptom was only reproduced on analog ports. PRI works with the same configuration.

  Workaround: Send the fax call through a PRI.

- CSCse50887

  Symptoms: MGCP IOS Gateway sees the following:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.

  and then:

  config term
  router(UNKNOWN-MODE)
  ```

  Or, the **show running-config** command output is only 5 bytes.

  Conditions: This symptom occurs under the following conditions:

  - Use MGCP with the **ccm-manager config** command
  - Have more than 20 MGCP end points (voice ports)
  - Run Cisco IOS Release 12.3(11)T or later releases
  - Reset device pool from Cisco CallManager

  Workaround: Add the **no ccm-manager config** command.

- CSCse59775

  Symptoms: A Cisco 3845 that is configured for voice may reload because of a software-forced crash that is caused by a Redzone memory corruption.

  Conditions: This symptom is observed on a Cisco 3845 that runs Cisco IOS interim Release 12.4(9.15).

  Workaround: There is no workaround.

- CSCse63494

  Symptoms: A router that is configured for Real-Time Protocol (RTP) may generate CPUHOG events and a traceback similar to the following:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (951/33),process = VOIP_RTCP.
  -Traceback= 0x60EA5A78 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  ```

  Alternatively, the router may unexpectedly reload and generate the following error message and traceback:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = VOIP_RTCP.
  -Traceback= 0x60EA5A58 0x60EA5C5C 0x614AD39C 0x614B55BC 0x614B59A0
  %Software-forced reload
  Preparing to dump core...
  ```

  Conditions: This symptom is observed on a Cisco router that receives a badly formatted RTP Control Protocol (RTCP) packet.

  Workaround: There is no workaround.

  Further Problem Description: Typically, the badly formatted RTCP packet is produced by a device that does not conform to the RFC 3550 standard.

- 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

- CSCsf03530

  Symptoms: A crash occurs on a router when it receives a message waiting indicator (MWI).

  Conditions: This symptom is observed when unity sends a notify to the gateway (GW), and the GW is suppose to convert to QSIG MWI. The GW crashes while running Cisco IOS Interim 12.4(9.18)T.

Workaround: There is no workaround.

- CSCsf31178

  Symptoms: HWIC-1GE-SFP may experience an issue where the Gig Ethernet interface is “stuck” in a Line UP/Protocol Down state. While in this state, the interface will not pass traffic. Clearing the interface or manually disabling/enabling will clear the condition. This symptom does not occur when 1000BASE-T SFP is used.

  Conditions: A Loss of Signal (for example, unplugging the cable) may cause the interface to become stuck in a Line UP/Protocol Down state.

  Workaround: Clearing the interface or manually shutting it down, then bringing it back up will clear the problem.

- CSCsf95938

  Symptoms: There is a leak in middle buffers after all Onboard DSPRM Pools are depleted.

  Conditions: This symptom is observed on a Cisco 3800 series router that is running Cisco IOS Release 12.4(7b) with support for CVP survivability.

  Workaround: There is no workaround.

- CSCsg05350

  Symptoms: A Cisco AS5850 crashes due to a chunk memory leak. See the following:

  ```
  Sep 9 13:07:04.428: %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  Sep 9 13:07:04.468: %DSMP-3-INTERNAL: Internal Error : NO MEMORY
  -Traceback= 0x601C66D4 0x61596938 0x61579DB0 0x61279508 0x6127C34C 0x6127DB50
  0x6127F6BC
  Sep 9 13:07:04.744: %MARVEL_HM-3-HM_RULES_RELOAD: Health Monitor causing a reload due
  to Fragmented processor_memory, Free processor_memory = 10402472 bytes, Largest
  processor_memory block = 522632 bytes
  ```

  Conditions: This symptom occurs when there is a chunk memory leak.

  Workaround: There is no workaround.

- 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.

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

  Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third party system.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek28604

  Symptoms: A Cisco device may reload (“System returned to ROM”) unexpectedly due to a memory leak in the ISDN L2 process.

  Conditions: This symptom is observed on a Cisco device that functions in a call manager-backhaul configuration after running under stress for about 24 hours.

  The output of the **show processes memory**, collected in regular intervals shows a memory leak in the ISDN L2 process. The amount of memory that is held by the ISDN L2 process will be very large and growing.

  Workaround: Enter the **isdn k 1** command on all backhauled serial interfaces.

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP.

  Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCse79994

  Symptoms: BRI Layer 2 remains in the ESTABLISH_AWAITING_TEI state instead of entering the MULTIPLE_FRAME_ESTABLISHED state.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.19a).

  Workaround: There is no workaround.

- CSCsf96318

  Symptom: QSIG (ISO) call back (ring back) fails between a Cisco 3745 router and a Cisco 1760 router.

  Conditions: The call back fails.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(3f)

Cisco IOS Release 12.4(3f) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3f) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek33076

  Symptoms: A RADIUS progress code is incorrectly reported for a call that fails at IPCP. The progress code reports that the Link Control Protocol (LCP) is the open state.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(3a) and that is configured for AAA.

Workaround: There is no workaround.

- CSCsb43767

  Symptoms: RADIUS stop packets that are sent to a RADIUS server may contain an incorrect value for the NAS-Port attribute (RADIUS IETF attribute 5). Information that is related to the asynchronous interface is not included in the Cisco-NAS-port VSA.

  Conditions: This symptom is observed on when a Cisco router sends stop packets to a RADIUS server via an asynchronous interface.

  Workaround: There is no workaround.

Miscellaneous

- CSCek34049

  Symptoms: A Cisco AS5850 that is configured for RPR+ may be unable to process more than 1990 MGCP voice calls. With more than 1990 MGCP voice calls, any of the following symptoms may occur:

  - Many DSP may time-out.
  - Active calls may hang.
  - Spurious memory accesses and tracebacks may be generated.
  - Incoming calls may be dropped.
  - NextPort SPE ports may be stuck in the “a” state.

  Conditions: These symptoms are observed on a Cisco AS5850 that runs Cisco IOS Release 12.4(3d) or Release 12.4(7a).

  Workaround: There is no workaround. A Cisco AS5850 that is used to its full capacity (4 CT3 worth of MGCP calls) may not scale beyond 1990 calls. When the symptoms have occurred, reload the Cisco AS5850.

- CSCek42816

  Symptoms: A voice gateway reloads while bulk calls are being processed.

  Conditions: The symptom is observed on a Cisco voice gateway that runs VXML applications that stream voice when the voice gateway receives prompts from an HTTP server.

  Workaround: Enter the **ivr prompt streamed none** command on the voice gateway.

- CSCsa70712

  Symptoms: When you reload a CMM in one slot, the CMM in another slot reloads too, and the console of the supervisor engine shows an “EarlRecoveryPatch Reset” error message for the CMM that you intentionally reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series when you enter the **reload** command via the console of the CMM.

  Workaround: Do not reload the CMM via its console. Rather, enter the **hw-module module** *slot number* **reset** command for the CMM on the supervisor engine.

- CSCsb23038

  Symptoms: While attempting performance/stress testing, a memory leak is experienced. The Terminating Gateway (TGW) could not be accessed through the console, the following message was output:

```
%% Low on memory; try again later.
```

The root cause is that the calls are being hung. SIP KPML was enabled on half of the dial-peers.

Conditions: This symptom is observed on a Cisco 3700 series router.

Workaround: Do not enable DTMF Relay on the dial peers, for example SIP KPML and others under heavy load conditions.

- CSCsb93407

  Symptoms: With H323 call service stopped, the router still listens on TCP port 1720 and completes connection attempts.

  Conditions: After H323 is disabled using the configuration commands:

  voice service voip

  h323

  call service stop

  Workaround: Access can be blocked by deploying an interface access list that blocks access to TCP port 1720 for traffic that is destined for any of the IP addresses of the router.

  For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document: http://www.cisco.com/warp/public/707/tacl.html.

  For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document: http://www.cisco.com/warp/public/707/iacl.html.

  For information about using control plane policing to block access to TCP port 1720, see the "Deploying Control Plane Policing White Paper": http://www.cisco.com/en/US/partner/products/ps6642/products_white_paper0900aecd804fa16a.shtml

- CSCsb99936

  Symptoms: The **show ephone** command reveals a call is stuck in the SEIZE state instead of progressing to the correct state during a call.

  Conditions: This symptom has been observed when an H.323 call is placed from CME to a non-CME H.323 endpoint.

  Workaround: There is no workaround.

- CSCsc97398

  Symptoms: The user information Layer 1 protocol may be included in the outgoing bearer capability and may be set to either G711 u-law or G711 A-law. Some PBXs may refuse the call because of this mismatch in the bearer capability.

  Conditions: This symptom is observed when a call is made from H.323 to ISDN with unrestricted digital information bearer capability.

  Workaround: There is no workaround.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that runs Cisco IOS Release 12.4(3b)B. The router has services 81, 82 and 90 configured. The only service that has a problem is 90. The packet traces indicate that the router is sometimes responding to "Here_I_Am" messages from the cache with "I_See_You" messages that contain an incorrect destination IP address. This situation leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3b) but may also affect other releases.

Workaround: There is no workaround.

- CSCsd37629

  Symptoms: Alignment errors and a bus error may occur on a Cisco platform that has the **ip inspect** command enabled.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: Disable the **ip inspect** command.

- CSCsd44118

  Symptoms: When running TCL/VXML applications that perform Media Play, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: This symptom is observed when Cisco IOS Media Play code forgets to release a memory at the end of Media Play.

  Workaround: There is no workaround. Contact Multiservices TAC (IOS) and request a patch.

- CSCsd66800

  Symptoms: A gateway-controlled T.38 fax relay between an MGCP gateway and another gateway may be disconnected unexpectedly.

  Conditions: This symptom is observed on a Cisco platform that is configured for Voice xGCP.

  Workaround: There is no workaround.

- CSCsd73526

  Symptoms: When a Cisco Content Services Switch (CSS) is used in a Customer Voice Portal (CVP) configuration, the Cisco IOS Voice Browser may be unable to play the media file. The CSS does send the HTTP Redirect message that points to the CVP, but the gateway does not react.

  Conditions: This symptom is observed on a Cisco AS5400HPX Universal Gateway after you have upgraded this platform from Cisco IOS Release 12.3(3a) to Release 12.4(3b). Other software components in the configuration are CVP 3.1 SR1, ICM 6.0, and Cisco CallManager 4.1(3)SR2.

  Workaround: Bypass the Cisco CSS, and point the VXML application directly to the CVP.

- CSCse56660

  Symptoms: Inbound calls to FXO ports on Cisco IOS VoIP gateways connect, but audio is not present.

  Conditions: With **caller-id enable** configured on FXO ports, the call will connect, but no audio is heard. When this occurs, the following error message can be seen at debug level:

  ```
  Jun 20 01:41:15.855: mbrd_e1t1_vic_connect: setup failed
  Jun 20 01:41:15.855: flex_dsprm_tdm_xconn: voice-port(0/0/1), dsp_channel
  (/0/2/0)
  ```

  Workaround: Disable caller id on the voice-port.

- CSCse68355

  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

Wide-Area Networking

- CSCek31660

  Symptoms: For VPDN sessions that are established with a LAC, the RADIUS progress code in the Stop record may be different from the RADIUS progress code in the Start record.

  Condition: This symptom is observed on a Cisco platform such as a Cisco AS5400 that runs Cisco IOS Release 12.4.(3a) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCek40618

  Symptoms: A router may crash by address error (load or instruction fetch) exception during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCsd19867

  Symptoms: BRI interfaces does not come up when you reload a router. You must enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected BRI interfaces to bring them up.

Conditions: This symptom is observed when you enter the **no isdn spoofing** command and reload the router.

Workaround: Disable the **no isdn spoofing** command.

Resolved Caveats—Cisco IOS Release 12.4(3e)

Cisco IOS Release 12.4(3e) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3e) but may be open in previous Cisco IOS releases.

- CSCef29090

  Symptoms: The throughput for TCPClear sessions on a Cisco AS5850 may not be as expected and there may be a slow response time.

  Conditions: This symptom is observed on a Cisco AS5850 with TCPclear sessions.

  Workaround: There is no workaround.

- 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

- CSCek38136

  Symptoms: When you deploy VoIP using PVDM2 / 5510 DSP modules, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with 5510 DSP modules. The symptom does not occur with 549 DSP modules.

  Workaround: There is no workaround.

- CSCsc03569

  Symptoms: Incoming and outgoing PSTN calls fail on a BRI interface.

  Conditions: This symptom has been observed on a Cisco 2620XM VoIP Gateway (MGCP) with Cisco IOS Release 12.4(2)T1 and a BRI Backhauled MGCP Gateway controlled by Cisco CallManager release 4.1(3)SR1.

  Workaround: There is no workaround.

- CSCsc12255

  Symptoms: When you deploy VoIP on an NM-HDV2 network module that is configured with a PVDM2-64 module, a hissing sound may be heard before the ringback tone starts on the calling side.

  Conditions: This symptom is observed only with an NM-HDV2 network module. Note that the symptom does not occur with an NM-HDV network module.

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.

- CSCsc95234

  Symptoms: When the **stcapp** global configuration command is enabled, the command is not accepted and the following error messages are generated:

  STCAPP: Internal error: Unable to create codec list... exiting stcapp shutdown initiated... waiting for calls to clear. stcapp shutdown complete.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(6.3) but may also affect Release 12.4T.

  Workaround: There is no workaround.

- CSCse15025

  Symptoms: An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

  When this problem occurs, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

  Because this issue impacts the signaling channels, it has been seen that calls either will not connect at all through impacted ports or in some cases when multiple simultaneous calls are present on adjacent voice ports/timeslots, the call may connect momentarily before being disconnected.

  If a problem occurs only on a single voice port, there is another problem, not this caveat (CSCse15025). PRI/BRI calls are not affected because PRI/BRI does not utilize the DSP for signaling purposes.

  When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port-number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41, and 42 is presented and some of the registers show double-octet information. See the example output (2) below.

  When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** port-number **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

  Further Problem Description: The changes in CSCse15025 includes changes in CSCsc11833 and CScsd90851. These changes have been shown to help mitigate this problem in the majority of cases.

There is a further detection and reset mechanism in CSCse15025 that will recover the DSP which is in this state. This mechanism will trigger immediately if the impacted voice port is an analog FXO port. For other voice ports, a delay in the detection will be present and it is possible to see the symptom of this problem before the recovery code triggers.

Note that the reset mechanism will cause any active calls utilizing the DSP in question to be dropped.

It is recommended if running with modules which can be impacted by this issue to upgrade to a release of software which contains the changes in CSCse15025. If the DSP is reset and the below output is seen, contact the TAC for further assistance. Note that this output is sent at debug level and it is recommended either to enable either syslog or logging buffered on the gateway.

Logging buffered on the gateway is enabled through the global command **logging buffered 50000 debug** as an example to set the logging buffered to use 50K bytes of processor memory for logging. The output of the log can be seen with the exec command **show log.**

Example output when detection and recovery code on gateway triggers:

```
*May 31 14:30:43.343: TDM pointers: 0100 0100 0115 0115. Deltas: 0001 0000.

*May 31 14:30:43.347: Received alarm indication from dsp(0/1)
0030 0000 0080 0000 0013 4100 2E2E 2F2E 2E2F 6D6F 6475 6C65 732F 7363 6865
6475 6C65 2F64 6562 7567 2E63 2833 3634 2900
*May 31 14:30:43.347: ../../modules/schedule/debug.c(364)

*May 31 14:30:43.347: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to Administrative Shutdown
*May 31 14:30:43.647: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to Administrative Shutdown
*May 31 14:30:43.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to Administrative Shutdown
*May 31 14:30:44.247: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to Administrative Shutdown

*May 31 14:30:48.147: Crash dump CLI may not be configured, not able to get
crash info, slot 0, dsp 1
*May 31 14:30:48.147: DSPDUMP - Recover slot 0 dsp 1
*May 31 14:30:48.147: DSPDUMP - ka sent 0, ka_cnt 51193, skip_ka 103079
*May 31 14:30:50.579: %DSPRM-5-UPDOWN: DSP 1 in slot 0, changed state to up
*May 31 14:30:50.947: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/0,
changed state to up
*May 31 14:30:51.219: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/1,
changed state to up
*May 31 14:30:51.371: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/2,
changed state to up
*May 31 14:30:51.523: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/0/3,
changed state to up
```

Following are command output examples:

1) Following is an example of normal output for FXO and EVM FXS ports.

For FXO ports, the value is usually 0x01 but for EVM FXS the value can be different. When you run the above-mentioned command, the expected output is that a single octet is displayed and only for register 39. (This command does not work for VIC-4FXS and VIC2-xFXS modules).

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#

Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x01
```

2) Following is an example of output for FXO and EVM FXS ports that indicates that the symptom has occurred. Note that the exact output for the register values is different, but when the symptom occurs, different lines with information are displayed as shown below:

```
router#term mon
router#test voice port 0/3/3 si-reg-read 39 1
router#

Values read from SiLabs Codec connected to DSP 0, channel 11:
------------------------------------------------------------
Register 39 = 0x5CB8
Register 40 = 0xFFFF
Register 41 = 0xFFFF
Register 42 = 0xFFFF
3) Following is an example of normal output for FXS and analog E&M modules. The values
that are listed in a normal case may be different, but only four registers of a single
octet should be displayed.
Values read from PEB2465 Codec connected to DSP 02 (channel 0):
------------------------------------------------------------
Extended Register Values (XR4..XR1) = 00, CC, 50, 11
```

4) Following is an example of output for FXS and analog E&M modules that indicates that the symptom has occurred.

```
Values read from PEB2x65 Codec connected to DSP 0, channel 1:
------------------------------------------------------------
Extended Register Values (XR4..XR1) = D001, B83C, 3FF1, 63AC
```

- CSCse34097

  Symptoms: When a voice call is made to one of the busy channels of BRI/PRI port, the call gets rejected, and then another call is made to the available port. The call gets connected, and the user hears an annoying hissing sound.

  Conditions: The procedure to recreate this scenario is the following:

```
Phone a & b ---OGW --VoIP --TGW(2611) --BRI/PRI --PBX -- phone c & d

Phone a calls phone c;
```

```
Phone b calls phone c;
Phone b calls phone d;

Phone d picks up and hears a hissing noise.
```

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(3d)

Cisco IOS Release 12.4(3d) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3d) but may be open in previous Cisco IOS releases.

Basic System Services

- CSCej18051

  Symptoms: Terminal window PPP clients may fail with Cisco Access servers.

  Conditions: This symptom has been observed on Cisco AS5400 gateways and Cisco AS5800 servers.

  Workaround: There is no workaround.

- CSCek27271

  Symptoms: The IPSLA test packets returned by the IPSLA responder for the UDP jitter operation have ToS value of 0 instead of the value configured for the operation. Because of this, the two IPSLA UDP jitter operations between same source and responder routers with just the different ToS configurations will report the same round trip time even though the expected values are different.

  Conditions: This symptom has been observed on the routers configured with an IP SLA User Datagram Protocol (UDP) jitter operation with microseconds precision and has the ToS value configured.

  Workaround: There is no workaround.

- CSCsb30875

  Symptoms: Active eRSC on a Cisco AS5850 gateway could hang after RPR+ failover, if the **aaa accounting system** command is configured.

  Conditions: The symptom has been observed under the following conditions:

  1. RPR+ failover occurred.
  2. Console connection window closed & reopened to the newly active eRSC after failover.

  Workaround: There are two workarounds.

  1. The eRSC hang will not happen if no attempt is made to close and reopen the console session with newly active eRSC after failover.
  2. Remove the **aaa accounting system** command from the configuration.

Interfaces and Bridging

- CSCei68284

  Symptoms: POS interfaces may remain in the up/down state after the router has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

  Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

IP Routing Protocols

- CSCeh80444

  Symptoms: A Cisco router may reload unexpectedly because of a bus error.

  Conditions: This symptom occurs when the router is configured with Stateful Failover of Network Address Translation (SNAT).

  Workaround: There is no workaround.

- CSCej62500

  Symptoms: NAT Stateful forces the router to crash when there is heavy traffic exchanged between two peer SNAT routers. When active routers come back and a DUMP request process occurs at the same time, entries time out all together. This generates a large number of ACK packet exchanges and the actual data structure which stores these ACKs cannot handle this amount.

  Conditions: This symptom has been observed with SNAT Active/Standby configuration using the SNAT UDP option. When the NAT table has a size larger than 10000 entries, all entries of the table time out together. This timeout generates high density of packet exchange due to SNAT flow control mechanism.

  Workaround: There is no workaround.

Miscellaneous

- CSCeh08363

  Symptoms: Bidirectional DTR does not function. The output of the **show dialer** command shows the incorrect dialer type.

  Conditions: This symptom is observed on a Cisco 3660 that runs Cisco IOS interim Release 12.3(12.9)T.

  Workaround: There is no workaround.

- CSCei28413

  Symptoms: A Cisco 3700 series that is configured for MGCP may crash because of a bus error and generate the following error message:

  System returned to ROM by bus error at PC 0x613F72D0, address 0xD0D0D15

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.4(1).

  Workaround: There is no workaround.

- 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

- CSCek33253

  Symptoms: NextPort modems that function in a T1 CAS signaling configuration do not dial all the DTMF digits successfully.

  Conditions: This symptom is observed when you enter valid DTMF digits such as # and * in dial a string.

  Workaround: Use MICA modems instead of NextPort modems.

  Alternate Workaround: Use ISDN PRI T1 instead of T1 CAS signaling.

- CSCsa63173

  Symptoms: CEF may not be updated with a new path label that is received from the BGP peer.

  If a router configured for BGP IPv4+labels multipath receives a BGP update that only changes the MPLS label for a non-bestpath multipath, the router fails to update the forwarding plane. This results in dropping or mis-branding the traffic.

  Conditions: In a IPv4+labels multipath setup, if a label is changed for the non-bestpath multipath and that is the only change in the new update received from the neighbor, the new label will not be programmed in forwarding, hence there will be label inconsistency between the BGP and the forwarding tables.

  Workaround: There is no workaround.

- CSCsa86572

  Symptoms: A large configuration in NVRAM on a primary or secondary RSP may become corrupted and the router may generate relevant warning messages during the execution of a **copy system:running-config nvram: startup-config** command.

  When you erase NVRAM by entering the **erase nvram** command and then enter the **copy system:running-config nvram: startup-config** command, the router may crash.

  Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

  Workaround: If the configuration file is significantly large, place a copy of the configuration file on a flash card or disk with ample space and enter the **boot config slot0:startup-config** command to force the startup configuration file to be read from the flash card.

  When you enter the **copy system:running-config nvram: startup-config** command, the current running configuration is saved to the flash card or disk and the configuration is auto-synchronized to the corresponding flash card on the secondary RSP.

  Caution: Do not remove the flash card while the **boot config slot0:startup-config** command is being executed.

- CSCsa97827

  Symptoms: A user who answers a call on a phone that is connected to an FXS port that has Calling Line ID (CLID) enabled for all voice gateways hears an audible squawk for a few seconds, followed by a normal media cut-through.

  Conditions: This symptom is observed on all voice gateways that run Cisco IOS Release 12.3(14) or a later release.

  Workaround: Wait for the analog phone to ring three or four times before you answer the phone.

- CSCsb04447

  Symptoms: A Cisco AS5400 does not generate a RADIUS stop record when a call disconnect is initiated by a modem on the Cisco AS5400.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.3(10a) or Release 12.3(12) and that is configured for PRI T1. The symptom does not occur when the remote end or a signal initiates the call disconnect.

  Workaround: There is no workaround.

- CSCsb25337

  Cisco devices running Cisco IOS which support voice and are not configured for Session Initiated Protocol (SIP) are vulnerable to a crash under yet to be determined conditions, but isolated to traffic destined to User Datagram Protocol (UDP) 5060. SIP is enabled by default on all Advanced images which support voice and do not contain the fix for CSCsb25337. Devices which are properly configured for SIP processing are not vulnerable to this issue. Workarounds exist to mitigate the effects of this problem. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

- CSCsb52900

  Symptoms: An inconsistency may occur in the outlabel information that is used by BGP and MPLS forwarding.

  Conditions: This symptom is observed when there are two route reflectors (RRs) that advertise the same route and when one of the routes is the best path. The symptom occurs when the following conditions are present:

  – The PE router that is the source restarts, causing the prefix to be readvertised with a new label.
  – The RR that forms the non-best path delays the withdrawal and readvertisement of the prefix, for example, because the RR has a heavy load.

  This situation causes BGP to function with the new label but MPLS forwarding to function with the old label.

  Workaround: Enter the **clear ip route** *network* command for the affected prefix.

- CSCsb76671

  Symptoms: Intermittent one-way audio (PSTN hears dead air) on inbound ISDN call through Cisco VoIP AS5850 gateway.

  Conditions: This symptom has been observed to occur with inbound ISDN calls with outbound SIP calls towards a Cisco MeetingPlace server. Numerous calls which are transferred via SIP REFER contribute to the gateway get into this state.

  Workaround: There is no workaround to prevent the gateway from getting into this state. Once in this state, reloading the gateway will help clear this condition for awhile.

- CSCsb79608

  Symptoms: The router may crash with DSP-related Decodes as PRI groups are added to the configuration.

  Conditions: This symptom has been observed on a Cisco AS5850 running Cisco IOS Release 12.4(3) in Split Mode. This symptom may occur on other Cisco AS5x00 series routers that utilize the same DSP module.

  Workaround: There is no workaround.

- CSCsb92920

  Symptoms: A router that is configured for IPHC may crash when you remove a service policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4 or 12.4T but may also occur on other platforms. The symptom occurs when you enter the following sequence of commands:

```
frame-relay switching

class-map match-all voip
 match protocol ip

policy-map p1
 class voip
  compress header ip

interface Serial6/0
 encapsulation frame-relay
 service-policy output p1
no shutdown

interface Serial6/0
 shutdown
 no  service-policy output p1
 no  encapsulation frame-relay
```

  Workaround: There is no workaround.

- CSCsc11833

  Symptoms:

  An analog or digital CAS port gets into a state where inbound and/or outbound calls through the port may no longer work.

  Conditions:

  This symptom has been seen on 2800/3800 gateways with analog or digital CAS ports which use PVDM2 DSP modules.

  It can take some time for the symptom to occur, but when it does occur, it impacts multiple ports which share the same signaling DSP. To see which DSP a port is using for signaling, check the output of the exec command **show voice dsp signa ling**. It has been observed to occur more often with those ports which use DSP 1 on the PVDM2 module for signaling.

  If a problem is noticed only on a single voice port, it would not be this issue.

  Since PRI/BRI does not utilize the DSP for signaling purposes, it is not impacted by this issue.

When the problem occurs and this is either on a VIC2-xFXO or EVM DID/FXS modulem, run 'test voice port <port #> si-reg-read 39 1' on one of the impacted ports. You need to run 'terminal monitor' first to see the output. The output typically should be a single octet value for register 39. When the problem happens, information for Registers 40, 41 and 42 is presented as well and some of the registers show double-octet information. See example output below.

If using FXS or analog E&M modules, use "test voice port <port #> codec-debug 10 1"' and compare the output. Again, the normal output will be single octet information for each register.

This test only needs to be run on one of the voice ports in this state to confirm if this is the issue being seen.

Workaround: There is no workaround to prevent this problem from occurring. Once in this state, a reload of the gateway is necessary to recover it.

Additional Information: If the problem being seen has been confirmed to be this issue, the software changes associated with this report will mitigate the problem in the majority of cases. It may still be possible to see the problem in some cases and if this is experienced contact the TAC for assistance.

- CSCsc12570

  Symptoms: The codec upspeed (i.e., G729 to G711ulaw) or downspeed (i.e., G711ulaw to G729) does not happen. Other packet stream-related call parameter changes, such as VAD and PLAYOUT, do not happen as expected.

  Conditions: This symptom has been observed when the codec type or other packet stream parameters are modified using MDCX or through the TDM side of the call module like VTSP.

  Workaround: There is no workaround.

- CSCsc27337

  Symptoms: A Cisco router may reload with a bus error.

  Conditions: This symptom has been observed when IPS is enabled with the MSN Messenger Client DNS Request signature or Yahoo Messenger Client DNS Request signature.

  Workaround: Delete the MSN Messenger Client DNS Request or Yahoo Messenger Client DNS Request signature with the **ip ips signature** *sig-id* **delete** command.

- CSCsc40236

  Symptoms: Incorrect outgoing labels are installed for BGP-IPv4 Multipath prefixes.

  Conditions: This symptom has been observed anytime that a label changes from a BGP-IPv4 Multipath peer.

  Workaround: Clearing the BGP neighbor should allow the correct labels to be installed.

- CSCsc40952

  Symptoms: Phones that are configured for Cisco VT Advantage feature will not register with SRST if they are engaged in SRST fallback operation.

  Conditions: This symptom is observed when using the following:

  - Cisco CallManager Version 5.0 (1.51.225)
  - Cisco 2600 product line for SRST
  - Cisco IOS Release 12.4

  Workaround: Unplug connection to Cisco VT Advantage.

- CSCsc44206

  Symptoms: A Cisco AS5400HPX that is running voice calls with Cisco IOS Release 12.4(3a) has higher CPU utilization than when running Cisco IOS Release 12.3(7) T based images.

Conditions: This behavior is for all types of voice call configurations.

Workaround: There is not workaround.

- CSCsc64985

  Symptoms: Whenever a voice call is completed, some errant informational messages are echoed to the console and any open Telnet sessions, even though no debugs are enabled. For example, for a DSPless POTS-to-POTS hairpin call, we might see:

```
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  PAK_SUPRESS
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  NSE_PAYLOAD
Nov 30 00:10:37.809 EST:                  SEQ_NUM_START
Nov 30 00:10:37.809 EST: Modify Nominator =
Nov 30 00:10:37.809 EST:                  NSE_PAYLOAD
Nov 30 00:10:37.809 EST:                  SEQ_NUM_START
```

  Conditions: This behavior is observed on any Cisco IOS voice gateway which is running a Cisco IOS version listed or implied by the “First Fixed-in Version” field of bug ID CSCsc12570 “mgcp does not switch codec (e.g. g711 to g729) during call”.

  Workaround: Use a build of Cisco IOS earlier than those listed or implied by the “First Fixed-in Version” field of bug ID CSCsc12570 “mgcp does not switch codec (e.g. g711 to g729) during call”.

- CSCsc68262

  Symptoms: A Cisco 2821 router may crash intermittently if the router switches Encapsulating Security Payload (ESP) packets.

  Conditions: This symptom has been observed on a Cisco 2821 router when switching ESP packets.

  Workaround: There is no workaround.

- CSCsc76407

  Symptoms: Router-originated packets that are subject to encryption are bypassing the Quality of Service (QoS) feature. This prevents QoS from giving priority to protocol packets (for example BGP), which in turn can cause these protocol packets to be dropped when the outgoing link is congested.

  Conditions: This symptom is observed when router-originated packets are IPSec encrypted.

  Workaround: Disable CEF and fast switching and use process switching.

- CSCsc80670

  Symptoms: The on-board FastEthernet 0/0 results in state “FastEthernet0/0 is up, line protocol is down” after a reload, power-up or a shutdown and no shutdown operation. This is verified when the FastEthernet 0/0 is connected to media converters in series.

  This symptom is not present if the Cisco 1718 and Cisco 2950 routers are connected directly, without any media converters in between. This symptom may not be present using a media converter from other vendors.

  Conditions: This symptom has been observed connecting the on-board port of a Cisco 17xx router that is running Cisco IOS Release 12.3(11)T to media converters in series.

  1718(fa0/0)--media converter----------media converter--(fa 0/1)2950

  This symptom has also been observed with Cisco IOS Release 12.4(5), which is the latest available image for this platform.

Workaround: Replace the media converter with one from another vendor.

- CSCsc81637

  Symptoms: A Cisco IOS VoIP gateway may reload unexpectedly.

  Conditions: This symptom is observed on a gateway such as a Cisco 2800 series or Cisco 3800 series that supports time-division multiplexing (TDM) hairpinning between voice modules. Under rare circumstances, the gateway may unexpectedly reload when a call is hairpinned between ports on the gateway.

  Workaround: There is no workaround.

- CSCsc94359

  Symptoms: The BGP table and CEF forwarding table may have mismatched labels for prefixes that are learnt from a remote PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when an eBGP session flap or route flap occurs on the remote PE router. A new label for the prefix is learnt from the remote PE router, but forwarding may not be updated properly.

  Workaround: There is no workaround. When the symptom has occurred, and to correct the situation, enter the **clear ip route vrf** *vrf-name network* command on the PE router that has mismatched labels.

- CSCsd30244

  Symptoms: The router crashes on busyout of a CT3 card.

  Conditions: This symptom has been observed only after the router is booted with no T1 configuration on the T3 controller.

  Workaround: There is no workaround.

- CSCsd39519

  Symptoms: The Media Gateway Control Protocol (MGCP) gateway hangs when getting voice calls from either the IP or the PSTN side in which a leg of the call is on a BRI Voice Interface Card (VIC). The gateway stops responding and does not process any traffic. The only way to bring the router back is to power-cycle it.

  Conditions: This problem can be seen for every call over a BRI VIC/WIC if the router is running Cisco IOS Release 12.4(4)T1 or later releases, but it is not seen when the router is running Cisco IOS Release 12.4(4)T.

  Workaround: For an MGCP GW with BRI interfaces, do not use the Cisco IOS release for later than Cisco IOS Release 12.4(4)T.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd46403

  Symptoms: Call comes into an E1 R2 line on a Cisco AS5350 or Cisco AS5400 and gets sent via H323 to an endpoint. The endpoint connects the call, but the Cisco AS5350 or Cisco AS5400 fails to TX ANSWERED on CAS leg resulting in a dead air call.

  Conditions: This symptom occurs on a Cisco AS5350 and a Cisco AS5400 that are running later releases than Cisco IOS Release 12.3(11)T9. Earlier releases are not affected. This symptom also occurs on a Cisco AS5350XM and a Cisco AS5400XM.

  Workaround: There is no a workaround.

- CSCsd58220

  Symptoms: The callee's phone rings continuously even after the caller goes on- hook.

  Conditions: When the caller goes on-hook, the gateway receives idle and does not recognize the idle. The call does not get disconnected and the callee keeps hearing the ringing tone continuously.

  Workaround: The callee has to pick up the phone for the call to be dropped.

- CSCsd58381

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

Wide-Area Networking

- CSCek28575

  Symptoms: A router reloads at the "process_modem_command" function during a test that involves asynchronous media.

  Conditions: This symptom is observed on a Cisco AS5400 but is not platform-dependent.

  Workaround: There is no workaround.

- CSCsc17673

  Symptoms: Using the **show caller full** or **show caller interface Virtual-Access XX full** commands on a PPPoE client interface causes the router to unexpectedly reload.

  Conditions: This symptom has been observed on routers using Cisco IOS Release 12.4(3.3) and later versions.

  Workaround: Avoid using those commands.

- CSCsc66612

  Symptoms: A Cisco router configured for Virtual Private Dialup Network (VPDN) may unexpectedly reload with Bus Error.

  Conditions: This symptom was observed on a Cisco7200VXR series router equipped with NPE-G1 processor card running Cisco IOS Release 12.3(14)T3.

  Workaround: There is no workaround.

Further Problem Description: The crash was preceded by “SYS-2-INPUT_GETBUF: Bad getbuffer” error messages.

Resolved Caveats—Cisco IOS Release 12.4(3c)

Cisco IOS Release 12.4(3c) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3c) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCek10384

  Symptoms: A Cisco 7200 router that is performing NAT could drop IPSec packets.

  Conditions: This symptom is observed on a Cisco 7200 router that is performing NAT functionality for IPSec transit packets. The router will NAT and forward the Inside to Outside IPSec (ESP) packets, but might drop the return IPSec packets from Outside to Inside.

  Workaround: Disable NAT for IPSec.

Miscellaneous

- CSCeh88604

  Symptoms: One or more VIP slot controllers reset.

  Conditions: This symptom is observed on a Cisco 7500 series when the **ip nbar protocol-discovery** command is enabled. The symptom may not be platform-dependent and may also occur on other platforms in a similar configuration.

  Workaround: Disable protocol discovery by entering the **no ip nbar protocol-discovery** command.

- CSCei33351

  Symptoms: A router that is configured for QoS crashes because of a bus error.

  Conditions: This symptom is observed when you bring up a session that has a policy map attached in both directions.

  Workaround: There is no workaround.

- CSCej13460

  Symptoms: The packets are not switched correctly using the Fast Switching with IPSec tunnel protection feature.

  Condition: This symptom has been observed in Cisco IOS Release 12.4(1b) when tunnel protection IPSec is configured and tunnel source interface has Fast- switching (but not CEF) configured.

  Workaround: Use CEF switching.

- CSCej42804

  Symptoms: A Cisco Gateway that is running Session Initiation Protocol (SIP) calls might run out of processor memory due to hung SIP calls.

  Conditions: Active and hung calls can be seen using the **show sip-ua calls** command. The following specific scenario will result in a hung call:

3. The gateway initiates an INVITE.
4. The gateway receives a 100/180 response.
5. The gateway sends a CANCEL.
6. The gateway receives the 200ok for the CANCEL.
7. The gateway receives an invalid final response for the INVITE (or no final response) and drops the message.

Each hung call will use a little more memory, and eventually the gateway will run out of memory.

Workaround: Downgrade to Cisco IOS Release 12.3(14)T3, Release 12.3(11)T6, Release 12.4(2)T1, or Release 12.4(1a).

- CSCej87817

  Symptoms: Policing is not dropping any packets after the offerred/sent rate is much above the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCsb42176

  Symptoms: A Cisco 7200 series may pause indefinitely when a neighbor reloads.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-POS-2OC3 port adapter.

  Workaround: There is no workaround.

- CSCsc12098

  Symptoms: The fix for busyout *slot* on the Cisco AS5400 platform causes build issues.

  Conditions: This symptom is observed on a Cisco AS5400 platform.

  Workaround: There is no workaround.

- CSCsc14106

  Symptoms: If the called party answers a call in the middle of a prompt, one- way voice occurs.

  Conditions: This symptom has been observed when a TCL application tried to play a prompt while a call is alerting and the call is answered before the prompt play is complete. If the call is answered after the prompt play is done, the symptom is not seen.

  Workaround: In the script, connection destroy and reconnect are handled to make sure a reconnect happens. This symptom is now fixed in Cisco IOS.

- CSCsc15366

  Symptoms: If a Media Gateway Control Protocol (MGCP) Create Connection (CRCX) request is received containing a request for a clear-channel codec, the Cisco 1760 router fails to find a matching codec, and the call fails.

  Conditions: This symptom has been observed on a Cisco 1760 router.

  Workaround: There is no workaround.

- CSCsc20149

  Symptoms: When you enter the **show voice call status** command five to six times in quick succession, the CPU use of a Cisco AS5850 reaches 99 percent. The Cisco AS5850 thereafter becomes very unstable in accepting incoming calls. This situation can be highly service-impacting under stress conditions.

Conditions: This symptom is observed on a Cisco AS5850 that is running a special image of Cisco IOS Release 12.3(11)T6 and occurs only when there are more than 900 H.323 voice calls.

Workaround: Do not enter the **show voice call status** command in a stress situation.

- CSCsc31082

  Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

  The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in **show frame-relay pvc** show the packets correctly.

  Conditions: A map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

  Workaround: There is no workaround.

- CSCsc39557

  Symptoms: Spurrious memory access errors are encountered that may cause a bus error crash.

  Conditions: This symptom is observed on a Cisco 2800 router that is utilizing voice and is running Cisco IOS Release 12.4(3). This appears to be seen only when caller-id is enabled on FXS ports.

  Workaround: Disable caller-id on any FXS ports.

- CSCsc51183

  Symptoms: A Cisco AS5850 may restart because of a software forced crash preceded by the following error:

  ```
  %SYS-6-STACKLOW: Stack for process VTSP running low, 0/12000
  ```

  Conditions: This symptom has been observed on Cisco IOS Release 12.3(11)T.

  Workaround: There is no workaround.

- CSCsc54584

  Symptoms: A standard ingress ACL for transit traffic does not function on an interface that is configured for MFR.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(11)T8 and that has an MFR bundle that is configured on a PA-MC-8TE1 port adapter. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsc66658

  Symptoms: Ping does not work if loopback is configured on the interface.

  Conditions: This symptom has been observed when loopback is configured.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCeg77994

  Symptoms: A LAC does not send an Accounting-Start RADIUS record to a RADIUS server for a user session.

Conditions: This symptom is observed on a Cisco platform that functions as a LAC and that runs Cisco IOS Release 12.3(14)T1 when a switchover occurs from one LNS to another LNS while the user session is brought up.

Workaround: There is no workaround.

- CSCsc49637

  Symptoms: If a PPPoE client session is timed out (e.g. due to a network outage), and a restart of the session is subsequently unsuccessful (e.g. because network outage persists or the PPPoE server has not timed out the prior session) and if the user then manually clears the session, then the router will no longer be able to bring up this session until a reload is performed.

  Conditions: This symptom has been observed when the PPPoE session is unexpectedly interrupted with Cisco IOS Release 12.3(8)T8 or Release 12.3(11) T5. The next feature also needs to be configured.

  pppoe-client dial-pool-number 1 dial-on-demand

  Workaround: Use the following procedure:

  1. Reload.
  2. Do not configure the DDR feature for the PPPoE session. This problem is limited to PPPoE client sessions using the DDR feature.

Resolved Caveats—Cisco IOS Release 12.4(3b)

Cisco IOS Release 12.4(3b) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3b) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCei93982

  Symptoms: A router that is running Cisco IOS may crash unexpectedly.

  Conditions: NAT must be enabled for this symptom to occur. The problem is seen when an application uses two well known ports: one for source and the other for destination. The outgoing translation is created, but on the return trip, using the previous source port as the destination, NAT may use the incorrect algorithm.

  For example, if a PPTP session is initiated to the well known port 1723 from source port 21 (FTP), then the outgoing packet will create a FTP translation (we look at source information when going from in->out). When the packet is returned, we again look at the source information to know what kind of packet this is. In this case we have the source port will be 1723, and NAT will assume this is a PPTP packet. This will try to perform PPTP NAT operations on a data structure that NAT built for a FTP packet and may lead to a crash.

  Workaround: There is no workaround.

- 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.

- CSCsb09852

  Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

  Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

  To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

  Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsb32141

  Symptoms: A router that is configured for Resource Reservation Protocol (RSVP) generates the following error messages on the console and then crashes:

  ```
  %LINK-0-REENTER: Fatal reentrancy, level=3, intfc=FastEthernet0/1
  -Process= "RSVP", ipl= 3, pid= 251
  %SYS-6-STACKLOW: Stack for process RSVP running low, 0/24000
  ```

  Conditions: This symptom is observed when the **ip rsvp bandwidth** and **service-policy output** commands are configured on the same interface and when the policy map for the service policy is configured with the **fair-queue** command.

  Workaround: Enter the **ip rsvp resource-provider** *none* command on the interface.

  Alternate Workaround: Enter the **ip rsvp bandwidth** *value* command and ensure that the *value* argument is equal to the value that is displayed on the “Available Bandwidth” line in the output of the **show interface** *interface* command plus the value that is shown in the “allocated” column in the output of the **show ip rsvp interface** command.

- CSCsb54823

  Symptoms: One router (R2) may begin sending updates to another router (R1) before R2 has received the BGP prefix list from R1.

  R1 does apply its inbound BGP prefix list so routes are denied if they need to be. However, R2 sends routes to R1 which are denied by R1.

  Conditions: This symptom is observed when both routers have negotiated a BGP outbound route filter (ORF) and when R1 sends its BGP prefix list to R2.

  Workaround: There is no workaround.

- CSCsc41694

  Symptoms: A router hangs while unconfiguring the BGP **no router bgp** command.

  Conditions: This symptom has been observed in Cisco AS5400 and Cisco AS5850 routers having the image c5400-js-mz.123-16.15

  Workaround: There is no workaround.

Miscellaneous

- CSCec16597

  Symptoms: Cisco CallManager controlled MGCP gateways configuration download function always configures “mgcp fax t38 inhibit”. If this is changed manually in the Cisco IOS CLI, the configuration download facility will change it back to “mgcp fax t38 inhibit”.

  This DDTS removes the code that automatically configures this line.

  If customers are using CCM MGCP fax relay between gateways that are running older Cisco IOS versions, and the Cisco IOS 12.4T version with this change, the fax connections originating from the gateways that are running previous Cisco IOS versions and terminating on the Cisco IOS Release 12.4T gateway will fail unless “mgcp fax t38 inhibit” is configured on the Cisco IOS Release 12.4T gateway.

  If all gateways in the customer network are running the new Cisco IOS 12.4T version with this fix, then they may configure which ever mode as desired.

  With the fix to CSCec16597, the configuration utility will neither add nor remove this CLI statement.

  Conditions: There are no conditions.

  Workaround: Use the following command to enable and disable Cisco fax relay:

  [no] ccm-manager fax protocol cisco

- CSCed94829

  Multiple Cisco products contain vulnerabilities in the processing of IPSec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for IPSec and can be repeatedly exploited to produce a denial of service.

  Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

  This advisory is posted at
  http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml.

- CSCef84174

  Symptoms: PPP forwarding may fail between two virtual access interfaces.

  Conditions: This symptom is observed on a Cisco AS5850 but is not platform-dependent.

  Workaround: Disable PPP multilink on the asynchronous interfaces.

- CSCeh09198

  Symptoms: A Cisco gateway that has the garbage detector (a tool that is used for debugging memory leaks) enabled may hang indefinitely.

Conditions: This symptom is observed when you enter the garbage detector-related **show memory debug leaks** command or **show memory debug incremental leaks** command.

Workaround: There is no workaround.

- CSCeh18306

  Symptoms: On a Cisco 2600-XM series that is configured with an AIM-ATM module, when one PVC is configured for ABR and another PVC is configured for another ATM class, CRC errors occur on the far end of the ATM link of the PVC that is configured for the other ATM class. This situation may occur because the PVC that is configured for ABR sends two RM cells in a row and overwrites some data of the PVC that is configured for the other ATM class

  Conditions: This symptom is observed on a Cisco 2651-XM that runs Cisco IOS Release 12.3 and that is configured with an AIM-ATM module. However, the symptom may not be platform-dependent and may occur on any platform that is configured with an AIM-ATM module.

  Workaround: Do not configure ABR on a PVC.

- CSCeh61467

  This caveat consists of the two symptoms, two conditions, and two workarounds:

  Symptom 1: After you have disabled MVPN on a VRF interface, the CPU use for the PIM process increases to 99 or 100 percent and remains at that level.

  Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases.

  Workaround 1: Before you disable MVPN on the VRF interface, enable and then disable multicast routing by entering the **ip multicast-routing vrf** *vrf-name* global configuration command followed by the **no ip multicast-routing vrf** *vrf-name* global configuration command.

  Symptom 2: A router that functions under stress and that is configured with a VRF interface may crash when an MDT group is removed from a remote PE router.

  Condition 2: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases, and occurs only when there are frequent link flaps or other multicast topology changes that affect the VRF interface.

  Workaround 2: There is no workaround.

- CSCei02275

  Symptoms: A Cisco router may reload when removing a Frame Relay map from a dial interface.

  Conditions: This symptom occurs when a dial (ISDN) interface is configured for Frame Relay encapsulation with a map that includes IP Header Compression.

  Workaround: There is no workaround.

- CSCei24086

  Symptoms: A Cisco AS5850 gateway that processes mixed traffic reloads unexpectedly after a few minutes of functioning under stress.

  Conditions: This symptom is observed on a Cisco AS5850 gateway that runs Cisco IOS interim Release 12.4(1.8)T and that is configured with voice traffic (H.323 and SIP) with PRI and CAS, Fax Relay T.38, and TDM Hairpinning.

  Workaround: There is no workaround.

- CSCei51142

  Symptoms: A CA server that is rebooted may reset the issued serial number to 1, thus re-issuing a certificate with the same serial number.

Conditions: This symptom is observed on Cisco routers such as a Cisco 1841 and Cisco 2811 that have a built-in hardware clock.

Workaround: There is no workaround.

- CSCei62522

  Symptoms: ISAKMP SA negotiation is not successful in aggressive mode.

  Condition: This symptom has been observed when testing Radius Tunnel Attribute with HUB and Spoke Scenario using Cisco IOS interim Release 12.4(3.3).

  Workaround: There is no workaround.

- CSCei62952

  Symptoms: After the PXF engine crashes or reloads, some prefixes are no longer routable.

  Conditions: This symptom is observed on a Cisco router after the PXF engine crashes or after you have entered the **microcode reload pxf** command.

  Workaround: Initiate an RP switchover or reboot the router.

- CSCei82163

  Symptoms: A Cisco AS5400 might not release all voice resources for an MGCP call after it is disconnected.

  Conditions: This symptom is observed on both the Cisco AS5400 and Cisco AS5850 platforms but is not platform dependent. The symptom is associated with the simultaneous disconnection of a large number of calls.

  Workaround: There is no workaround.

- CSCej10160

  Symptoms: A spurious memory access is generated on a Cisco 3700 series, causing IPMC voice traffic to be dropped temporarily.

  Conditions: This symptom is observed on a Cisco 3700 series that has DSP-related features enabled and that has Cisco Land Mobile Radio (LMR) features configured on the voice ports.

  Workaround: There is no workaround.

- CSCej20505

  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

- CSCej50928

  Symptoms: Media Gateway Control Protocol (MGCP) calls fail to land in timeslots 16-31 on E1 controllers.

  Conditions: This symptom is observed in a Cisco AS5850 platform that is running a Cisco IOS Release 12.4(5) image. This symptom is not observed if OGW is a Cisco AS5400 platform. This was not observed in a Cisco IOS Release 12.4(3.8) image. This may be service impacting as only half of the timeslots can be used for generating calls.

  Workaround: There is no workaround.

- CSCej83415

  Symptoms: A Cisco IOS gateway might crash while running voice calls.

  Conditions: This symptom is observed under high stress/high CPU where race conditions in Cisco IOS are more likely to occur. These race conditions can result in a MIBS data base corruption or RTP memory corruption resulting in a crash.

  Workaround: There is no workaround.

- CSCek01162

  Symptoms: When removing the OSPF IPsec authentication configuration from CLI in IPV6, an alignment traceback will be seen pointing back to crypto_ikmp_peer_is_dead.

  Conditions: This symptom occurs when OSPF IPsec authentication (IPV6) is configured and removed.

  Workaround: There is no workaround.

- CSCin97574

  Symptoms: Service Selection Gateway (SSG) sends invalid Radius Access Reject packet to a network access server (NAS).

  Conditions: This symptom is seen with SSG in radius proxy mode when AAA server is unreachable.

  Workaround: There is no workaround.

- CSCin97815

  Symptoms: When performing the **show policy-map interface MFR** command, the counters do not increment.

  The counters in **show policy-map interface MFR** do not increment for any type/class of service. Even the class-default shows 0 packets. The counters in the **show frame-relay pvc** command show the packets correctly.

  Conditions: A map-class is configured under an MFR (FRF.16) bundle (sub- interface). This map-class consists of both an input and output service-policy.

  Workaround: There is no workaround.

- CSCsa53334

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  – Fragmented IP packets may be used to evade signature inspection.

  – IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml.

- CSCsa82945

  Symptoms: A router crashes because of a bus error when ICMP or UDP packets that are larger than 1393 bytes are transmitted through an IPSec tunnel.

  Conditions: This symptom is observed when a policy map and crypto map are applied to the tunnel interface.

  Workaround: Remove the policy map.

- CSCsa86390

  Symptoms: A router generates an ALIGN-3-TRACE traceback and a DSPDUMP in its log, and the output of the **show align** command shows that the spurious access counter is not zero.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 2800 series when an error message is generated during stress calls.

  Workaround: There is no workaround.

- CSCsb39237

  Symptoms: When using a Cisco 3845 router with Cisco IOS Release 12.4 and entering the **show ip inspect statistics** command, the number for the half-open session kept increasing, never decreasing. If it reaches the maximum, then no one can establish any new SSL session. It can cause a potential router crash.

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(1). This has been seen when ICMP inspection is enabled with the **ip inspect name** *name* **icmp**.

  Workaround: Increase the half-open session limit with the **ip inspect max-incomplete high** command.

- CSCsb51663

  Symptoms: The SNMP process hangs while a QoS MIB object is queried.

  Conditions: This symptom is observed when the execution of a QoS **show** command is in the “More” state while the QoS MIB object is queried. The SNMP process resumes when the **show** command is finished. Depending on the SNMP configuration, different symptoms may occur while the SNMP process is waiting for the QoS **show** command to finish.

  Workaround:

  Don’t leave the **show policy-map** command or the **show class-map** in the more state or prior to executing one of these commands issue the exec command **term len 0** and after the show command is complete issue the exec command **term len 24**.

- CSCsb54961

  Symptoms: A Cisco gateway may fail to initiate a T.38 call to a third party gateway. When the third party gateway sends T.38 open logical channel to the Cisco gateway, no open logical channel acknowledgement is sent by the Cisco gateway. After waiting for 30 seconds for T.38 open logical channel acknowledgement, the third party gateway closes its T.38 open logical channel.

  Conditions: This happens when T.38 fax relay calls are originated or terminated on a Cisco gateway that is running Cisco IOS Release 12.3(4)T and later releases.

  Workaround: There is no workaround.

- CSCsb56867

  Symptoms: A Cisco IOS VoIP gateway may reload unexpectedly.

  Conditions: This symptom is observed when an attempt is made to poll some SNMP information from the gateway while the gateway processes voice and fax calls.

  Workaround: Apply the following configuration changes. The following commands would prevent query of any callActive OIDs:

  ```
  conf t
  snmp-server view <viewname> callActive excluded
  end
  wr
  ```

  Further Problem Description:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- CSCsb58313

  Symptoms: After running a few days, assertion failed at WA_NP_QWRITE and then crashed.

  Conditions: This symptom occurs when running the **show diag** command at high CPU.

  Workaround: Do not run the **show diag** command.

- CSCsb65056

  Symptoms: A PPP connection may remain active after the idle-timer zeroes out. This situation may affect other services that rely on the termination of the PPP connection. Also, an incorrect redirection may occur.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG when the host object is disconnected but the PPP connection remains active.

  Workaround: There is no workaround.

  Further Problem Description: After the host idle-timeout/user idle-timeout in the output of the related virtual access interface, you can troubleshoot the situation through the **debug ssg events** command.

- CSCsb67234

  Symptoms: L3 communication with the router through the VLAN interface (SVI) for non-default VLAN may break. For example, pings from VLAN interface to any device connected to switch-port/s in that VLAN, may not go through. If the **show mac-address-table** executive mode command is executed, entry marked as “Self” will not be seen for the non-default VLAN SVI (It would be seen only for VLAN1 SVI).

  See the following:

  ```
  1841#
  1841#sh mac-address-table
  Destination Address  Address Type  VLAN  Destination Port
  -------------------  ------------  ----  --------------------
  0013.c45d.e300          Self          1     Vlan1
  0013.c45d.e300          Dynamic     180     Vlan180
  00ff.ff30.0408          Dynamic     180     FastEthernet0/1/0
  0013.c45d.e300          Dynamic     182     Vlan182
  ```

```
1841#
```

Conditions: This symptom is observed on a router having a HWIC ESW module and non-default VLAN and corresponding SVI configured on the router. The router is reloaded.

Workaround: Do a **shut** command followed by the **no shut** command on the VLAN interface.

- CSCsb67539

  Symptoms: A Voice Gateway crashes when running under a heavy voice call load.

  Conditions: This symptom is observed on a Voice Gateway that is running Cisco IOS Release 12.3(11)T6. The gateway is under heavy voice call load with access to media/application documents residing on local gateway flash, http and tftp servers.

  Workaround: The following is not quite a workaround:

  call threshold global *cpu-5sec* **low** *value* **high** *value*

  For example:

  call threshold global *cpu-5sec* **low** *50* **high** *70*

  The CLI can ease the CPU load on the gateway by reducing the probability for a crash.

- CSCsb72138

  Symptoms: A Foreign Exchange Station (FXS) port may lock up after having functioned fine for a long time.

  Conditions: This symptom is observed on a Cisco 2821 that runs Cisco IOS Release 12.3(11)T5. This symptom typically occurs when fax lines are configured on the FXS port.

  Workaround: There is no workaround.

- CSCsb77885

  Symptoms: IKE negotiation will fail. Any tunnel that requires IKE to successfully negotiate a security association will not work.

  Conditions: This symptom occurs when authentication for IKE is configured as RSA encryption (authentication rsa-encr).

  Workaround: There is no workaround.

- CSCsb85136

  Symptoms: When running TCL/VxML applications that perform Media Playing, the gateway (GW) leaks memory. If the GW continues to run, eventually it will run out of memory. When there is no memory left on the GW, the GW could crash.

  Conditions: Cisco IOS Media Play code was forgetting to release a memory at the end of media play.

  Workaround: Upgrade to Cisco IOS Release IOS 12.4(3b) if available. If not, contact Multiservices TAC (IOS) and request a patch.

- CSCsb90264

  Symptoms: Cisco AS5400 and AS5350 T1 CAS calls fail with “no users answer,” and a traceback is seen at vtsp_tsp_call_setup_ind, along with the following error:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
  ```

  Conditions: This problem is seen when making CAS calls in Cisco AS5400 and AS5350 platforms.

  Workaround: There is no workaround.

- CSCsb97185

  Symptoms: A router configured with a 36-port EtherSwitch Module may reload due to memory corruption in the I/O memory pool.

  Conditions: The router must have a 36-port ESW module.

  Workaround: Disable the **ip igmp snooping** command.

```
Router(config)#no ip igmp snooping
Router#show ip igmp snooping
vlan 1
----------
  IGMP snooping is globally disabled
  IGMP snooping is disabled on this Vlan
  IGMP snooping immediate-leave is disabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

- CSCsc00587

  Symptoms: PRI backhauled to MGCP cannot fallback into h323 mode for SRST as there is a hung call. It can be seen in the **show call active voice brief** command but if there is no calls there, definitely check the**show voice vtsp call** command. There will be a call in "S_WAIT_RELEASE" state and cannot be cleared even though ISDN status shows no active calls on that PRI.

  Conditions: This symptom is normally seen when connection from a gateway to CCM flaps. If a call hits the gateway during a transition (fallback switchover or vice versa), the call gets stuck and causes all other PRIs to clock up. The PRI is able to be backhauled to CCM with a hung call but it is not able to fallback into SRST (gateway terminated). With just one call hung, all other backhauled PRIs are affected and cannot fallback in h323. Calls inbound get a "fast busy--- isdn setup" message and is ignored by the gateway as it thinks PRI is still backhauled, so the PRIs are in limbo.

  Workaround: Reload the router.

- CSCsc09246

  Symptoms: The following commands used for detecting memory leaks would crash the router which uses external memory such as the RPM-XF platforms.

  show memory debug leaks show memory debug leaks chunks show memory debug leaks largest show memory debug leaks summary

  Conditions: This symptom has been observed on the RPM-XF cards using Cisco IOS interim Release 12.4(4.6).

  Workaround: There is no workaround.

- CSCsc13844

  Symptoms: After load "flash:c2600-entservicesk9-mz.123-11.T7.bin", the E1 controller is missing from the **snmpwalk** command of IF-MIB.

  Conditions: This symptom has been observed on a Cisco2621XM.

  Workaround: There is no workaround.

- CSCsc21674

  Symptoms: PSTN is sending in an "*" and the router is reading it in as a "D". PSTN is also sending in a "#" and router is reading it in as an "*".

  Conditions: This symptom has been observed on an MGCP T1-CAS gateway connected to Cisco CallManager doing MF and using Cisco IOS Release 12.3(8)T11, Release 12.3(11)T7, or Release 12.3(14)T4.

Workaround: There is no workaround.

- CSCsc41913

  Symptoms: A Cisco IOS gateway using Cisco IOS Release 12.3(8)T or later versions will use an ephemeral port to send a response to any SIP request. This may not work with port restricted NAT, which is expecting a response on the same connection as the one on which the request was sent and may drop the response.

  Conditions: This symptom is observed on a Cisco IOS gateway with Cisco IOS Release 12.3(8)T or later releases and a port restricted NAT.

  Workaround: There is no workaround.

- CSCsc44237

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: A switch or router that is either configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

  The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

  Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory.

  The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.

  Condition 1: This symptom is observed on a Cisco Catalyst 6500 series, Cisco 7500 series, and Cisco 7600 series.

  Condition 2: This symptom observed on a Cisco 2811 and Cisco 3845 and occurs only in Cisco IOS Release 12.2(30)S, interim Release 12.4(2.10), and interim Release 12.4(2.10)T, or in any later releases.

  Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

  Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf** *vrf-name* command is configured, enter the **ip vrf forwarding** *vrf-name* command on at least one interface that has PIM enabled.

Protocol Translation

- CSCei15942

  Symptoms: You may not be able to download a complete file from an FTP during a V.120 session.

  Conditions: This symptom is observed on a Cisco AS5400 and Cisco AS5850 that runs Cisco IOS Release 12.2(15)ZK6 or Release 12.3(11)T5. The symptom could also occur in other releases such as Release 12.3 or Release 12.4.

  Workaround: This problem can be circumvented by disabling the negotiation of multilink on the client adapter or the router. Alternatively, configuring **ppp multilink queue depth fifo 10** on the Virtual-Template interface should allow for a successful FTP download.

Wide-Area Networking

- CSCei11919

  Symptoms: A dialed circuit that carries a PPP connection over a tunnel between an LNS and a LAC is not dropped when the tunnel is reset.

  Conditions: This symptom is observed when you enter the **clear vpdn all** command, when the LNS reloads, when the IP link between the LSN and LAC is disrupted, or when any other event occurs that causes the tunnel to be reset.

  Workaround: There is no workaround.

- CSCej45061

  Symptoms: Attempts to remove a PRI group fail.

  Conditions: This symptom is observed when an NFAS group has group number 0 and when you attempt to remove a FAS PRI group.

  Workaround: Shut down the NFAS group before you remove the FAS PRI group.

- CSCej73049

  Symptoms: AAA method may fail on calls in the Cisco IOS 12.3(11)T releases.

  Conditions: This symptom was observied on a Cisco AS5850 that was running Cisco IOS Release 12.3(11)T8 but is not platform dependent.

  Workaround: There is no workaround.

- CSCsa55747

  Symptoms: The RADIUS L2TP-specific disconnect code value for the Ascend-Disconnect-Cause RADIUS attribute (195) is incorrectly generated as 607 instead of 605.

  Conditions: This symptom is observed when an L2TP tunnel setup failure occurs between a LAC and an LNS.

  Workaround: There is no workaround.

- CSCsb89292

  Symptoms: ISDN NFAS failover issues are observed in Cisco IOS Release 12.3(11) T7. If the primary NFAS d-channel is bounced, the switch sees some of the b- channels in “remote busy” (RMB).

  Conditions: This symptom only happens when the primary NFAS d-channel is bounced.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(3a)

Cisco IOS Release 12.4(3a) is a rebuild release for Cisco IOS Release 12.4(3). The caveats in this section are resolved in Cisco IOS Release 12.4(3a) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCei06089

  Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

- CSCsb13988

  Symptoms: A router that is configured for NAT may crash because of a bus error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(9a) but is not platform-specific. The crash occurs while NAT attempts to translate an IP address in an H.323 RAS messages that does not contain an IP address.

  Workaround: Disable H.323 RAS in NAT by entering the **no ip nat service ras** command. If you must use H.323 RAS in NAT, there is no workaround.

Miscellaneous

- CSCeh63526

  Symptoms: A router crashes at the insp_inspection function.

  Conditions: This symptom is observed when the inspection rule is removed and re-added to an interface while traffic passes through the interface.

  Workaround: There is no workaround.

- CSCei37299

  Symptoms: A VPN hub router may reload when you enter the **clear crypto session remote** *ip-address* command.

  Conditions: This symptom is observed after a remote peer disconnects ungracefully (that is, the peer is suddenly powered-off or the LAN cable is disconnected) and immediately reconnects to the VPN hub router with a different public address.

  Workaround: Do not enter the **clear crypto session remote** *ip-address* command. Rather, enter the **clear crypto sa** command.

- 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.

- CSCei79855

  Symptoms: When Cisco IOS software is secured using “secure boot” commands and after formatting the disk, the **show disk** command will not display the secured image and the corresponding configurations in the output.

  Conditions: This symptom occurs when securing the Cisco IOS software using the **secure boot-config** and the **secure boot- image** commands and formatting the disk.

Workaround: There is no workaround.

- CSCsb40055

  Symptoms: A service name is absent from a service authorization request packet that is sent by an SSG to a prepaid server.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCeg20283

  Symptoms: E1R2 SS7 calls fail to come up when more than one call is made with the following ISDN error:

  ```
  ISDN Se1/6:15 SC **ERROR**: call_connect: call_id not found, rejecting call
  ISDN  **ERROR**: Module-CCPRI  Function-CCPCC_CallConnected  Error-Unknown
  event received in message from L3 or Host:  4F
  ```

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(11)T.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(3)

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

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.

- 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.

- 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.

- CSCef39130

  Symptoms: A router crashes when you enter the **redundancy force-switchover** command on the master RSP to initiate a switchover to the slave RSP.

  Conditions: This symptom is observed on a Cisco 7500 series that has two RSPs and that is configured for SSO.

  Workaround: There is no workaround.

- CSCeg52924

  Symptoms: When TACACS+ accounting or authorization is configured, many CPU cycles are consumed, messages are not sent, and the platform is unusable.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 when TACACS+ accounting, authentication, or authorization is enabled with a faulty server and when the server sends unsolicited data while the socket is being set up.

  Workaround: Disable TACACS+.

- CSCeg61032

  Symptoms: A memory leak may occur or all memory may be allocated but not freed when an internal OS registry call is made from a process.

  Conditions: This symptom is observed on a Cisco platform that is configured for MPLS.

  Workaround: There is no workaround.

- CSCeg62206

  Symptoms: High CPU utilization may occur during the TPLUS process on a platform.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(6c) and that is configured for TACACS.

  Workaround: There is no workaround.

- CSCeh04755

  Symptoms: When you reload a router by entering the **reload** command, the router may unexpectedly enter the ROMmon mode and generate the following error message:

  ```
  %SYS-5-RELOAD: Reload requested by console. Reload Reason:Reload command. monitor:
  command "boot" aborted due to user interrupt rommon 1 >
  ```

  Conditions: This symptom is observed only on a Cisco 7200 that is configured with an NPE-G1, and on UBR7246VXR with UBR-NPE-G1

  Workaround: Enter the **confreg 0x2002** command.

- CSCeh20434

  Symptoms: A router crashes when an RTR probe is configured.

  Conditions: This symptom is observed when the RTR and the fallback system process are not synchronized. For each RTR probe, the fallback system creates a cache entry and keeps it for cache timeout. During the cache timeout, the fallback system process sends an event to RTR and frees the entry, but RTR sends an event after the cache entry is deleted.

  Workaround: There is no workaround. Note that caveat CSCeg89043 fixes the problem from the fallback system process side but not the above-mentioned symptom.

- CSCeh31423

  Symptoms: Authentication via a TACACS server may fail.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA authentication.

  Workaround: There is no workaround.

- CSCeh47604

  Symptoms: An OER border component does not sent passive updates for OER prefixes, preventing the prefixes from being controlled. The prefixes cycle from the default state to the hold-down state back to the default state.

  Conditions: This symptom is observed when NetFlow is configured and when the mode monitor is configured to be “passive” or “both”.

  Workaround: Configure the mode monitor to be “active”. The functionality of the mode monitor is limited to the “active” mode only.

- CSCeh64791

  Symptoms: A memory leak may occur when you delete a RADIUS server group.

  Conditions: This symptom is observed when the server is configured with a key.

  Workaround: There is no workaround.

- CSCeh65692

  Symptoms: Spurious memory access errors and tracebacks may be generated on a Cisco AS5800.

  Condition: This symptom is observed on a Cisco AS5800 that processes TCPclear calls.

  Workaround: There is no workaround.

- CSCeh71577

  Symptoms: A Cisco 7200 series does not load an image and generates a traceback.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(1), that is configured with an NPE, and that has the L3 cache disabled.

  Workaround: Enable the L3 cache by entering the **no l3 cache disable** command.

- CSCeh71837

  Symptoms: The CPU use of a NAS may reach 100 percent when you test Redirect Number support by using a TACACS+ accounting VSA.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(1.6), that functions as a NAS, and that has the **aaa nas redirected-station** command enabled. The symptom may also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCeh82694

  Symptoms: A router crashes when an snmpwalk is performed on the ifTable.

  Conditions: This symptom is observed when an interface that is registered for high capacity (HC) counters deregisters directly.

  Workaround: Disable SNMP or do not poll the ifTable through SNMP.

- CSCin88970

  Symptoms: Using snmpwalk on the CISCO-ENTITY-FRU-CONTROL-MIB causes a platform to crash. When the platform does not support the cefcFRUPowerStatusTable and cefcFRUPowerSupplyGroupTable of the CISCO-ENTITY-FRU-CONTROL-MIB, the system may pause indefinitely.

  Conditions: These symptoms are observed on a Cisco platform that has SNMP enabled.

  Workaround: Either exclude the CISCO-ENTITY-FRU-CONTROL-MIB from the view or exclude the cefcFRUPowerStatusTable and cefcFRUPowerSupplyGroupTable from the view.

  Further Problem Description: Most platforms do not support the CISCO-ENTITY-FRU-CONTROL-MIB.

- CSCin90842

  Symptoms: Memory allocations fail on the gateway though there is enough free memory. If this failure happens in ISDN, the gateway crashes subsequently.

  Conditions: This symptom has been observed when the **H323 aaa accounting** command is enabled.

  Workaround: There is no workaround.

  Further Problem Description: Memory allocations for a block of 3k bytes fail with memory fragmentation as the cause. When this failure occurs, there is approximately 20MB of free memory on a gateway with 220MB of processor memory.

- CSCin92442

  Symptoms: You may not be able to establish an outbound Telnet connection on a router, nor may you be able to establish a reverse Telnet connection into a modem from the router console.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or interim Release 12.4(2.2)T but may also occur in Release 12.3.

  Workaround: There is no workaround.

- CSCsa92212

  Symptoms: A Path Echo Service Assurance Agent (SAA) operation misses hops.

  Conditions: This symptom is observed when you perform a Path Echo SSA operation from a Cisco router that runs Cisco IOS Release 12.3.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2.

- CSCsa92394

  Symptoms: A router may crash while loading the image for a secondary RSP from a disk during the boot process.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with redundant RSPs when the **hw-module slot** *slot-number* **image disk0:** *image* command is configured.

  Workaround: There is no workaround.

- CSCsb03401

  Symptoms: You cannot open a specific port on a Cisco IOS IP SLA responder.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T1 or Release 12.4 when you attempt to open a specific port on the responder instead of using normal control protocol.

  Workaround: Use normal control protocol.

- CSCsb27960

  Symptoms: When the local method is used at the beginning of a PPP authentication method list and when a user does not exist in the local database, failover to the next method in the method list does not occur. This situation prevents users that are listed in the database of a RADIUS or TACACS+ server from being authenticated.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA.

  Workaround: Temporarily remove the local method from the beginning of the method list.

EXEC and Configuration Parser

- CSCsb08994

  Symptoms: The **test ip** command returns an ambiguous command error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS interim Release 12.4(2.5) or interim Release 12.4(2.2)T and that is configured with an NPE-G1 (revision B) processor.

  Workaround: There is no workaround.

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.

Interfaces and Bridging

- CSCef01220

  Symptoms: A Versatile Interface Processors (VIP) with a PA-MC-8TE1 port adapter may report its memory size as unknown even though the VIP appears to function normally, and Distributed Multicast Fast Switching (DMFS) may fail to function properly.

  Conditions: This symptom is observed on a Cisco 7500 series when any of the following conditions are present:

  – The mode of the controller of the PA-MC-8TE1 port adapter is not set to T1 or E1 and you insert or remove another VIP with any port adapter via an OIR.

  – Irrespective of whether or not the mode of the controller of the PA-MC-8TE1 port adapter is set to T1 or E1, you insert or remove a standby RSP via an OIR.

  Workaround: Enter the **card type** {**t1** | **e1**} *slot* [*bay*] command on the PA-MC-8TE1+ port adapter and ensure that none of the controllers on this port adapter are shut down.

- CSCef49896

  Symptoms: Packets that enter an interface that is configured for IP may not be switched via dCEF.

  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 affected interface.

  ALternate Workaround: If many interfaces are affected, reload all port adapters by entering the **microcode reload** command on the control plane of the RSP.

- CSCef82084

  Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

  Conditions: This symptom is observed after you have configured a new MLP interface and a new EBGP neighbor.

  Workaround: There is no workaround.

- CSCeg17576

  Symptoms: Traffic loss may occur when you enter the **ip multicast-routing** and **ip pim** commands on an Ethernet interface that is already configured for Xconnect.

  Conditions: This symptom is observed only on a Cisco 7200 series and Cisco 7500 series.

  Workaround: To enable Xconnect traffic to resume, unconfigure and reconfigure the Xconnect statement on the Ethernet interface.

- CSCeh10624

  Symptoms: A Cisco 7206VXR may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(10a) and that is configured with an NPE-G1 and a couple of PA-MC-8TE1+ port adapters. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeh43864

  Symptoms: The line protocol on the POS interface of a PA-POS-OC3 port adapter flaps continuously.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.3(14.10) but may also occur in other releases.

  Workaround: There is no workaround.

- CSCei08289

  Symptoms: The transmit rate is higher than the configured committed information rate (CIR), causing the network to drop frames.

  Conditions: This symptom is observed only when traffic is process-switched and when software payload compression and header compression are configured.

  Workaround: Enable either CEF or fast-switching. If process-switching must be used, add a compression adaptor and configure FRF9 data compression instead of packet-by-packet payload compression. You can enable FRF9 data compression in the following ways:

  – On a point-to-point interface: enter the following command in interface configuration mode:

    frame-relay payload-compression frf9 stac

  – On a multipoint interface: enter the following command in interface configuration mode:

frame-relay map ip *ip-address dlci* **payload-compression frf9 stac**

Further Problem Description: We do not recommend process-switching in combination with software payload compression because it is not possible to provide latency guarantees.

- 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.

- CSCin75573

  Symptoms: When you perform an OIR of a PA-MC-8TE1+ or PA-MC-8E1 port adapter, the following error message and traceback may be generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x60379D34 reading 0xD8 %
  ALIGN-3-TRACE: -Traceback= 60379D34 604F1CFC 60BD0664 6032B93C 6039A0CC 6010A908
  6032AA7C 6032EBAC
  ```

  Conditions: This symptom is observed on a Cisco router when the port adapter is configured for QOS on an egress serial interface and traffic is flowing through this interface.

  Workaround: There is no workaround.

- CSCin89590

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: On the RSP console, the link status of a Fast Ethernet (FE) interface is shown as UP/DOWN, but on the VIP console, the link status of the same interface is shown as UP/UP.

     Condition 1: This symptom is observed on a Cisco 7500 series until a packet that is received on the FE interface reaches the RSP.

     Workaround 1: There is no workaround.

  2. Symptom 2: An FE interface is in the UP/UP state but the output of the **show ip route** command does not show any routes through the interface.

     Condition 1: This symptom is observed on a Cisco 7500 series.

     Workaround 2: Enter the **clear ip route** command on the affected FE interface. Note that doing so causes all routes to be relearned.

- CSCsa46510

  Symptoms: When you enter the **microcode reload** command, an error message similar to the following and a traceback may be generated:

  ```
  RSP-3-RESTART: interface Serial3/0/1/4:0, not transmitting
  -Traceback= 404436B4 4044DE10
  ```

  Conditions: This symptom is observed on a Cisco 7500 that is configured with a E1, T1, E3, or T3 port adapter.

  Workaround: There is no workaround.

- CSCsa83897

  Symptoms: A channelized T3 port adapter cannot detect C-bit errors and does not shut down after continuous C-bit errors.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a channelized T3 port adapter.

Workaround: There is no workaround.

- CSCsa87986

  Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that "protocol reject" packets are received from the remote end.

  Conditions: This symptom is observed on a Cisco 7500 series that has only one OC3 POS port adaptor per VIP and that is configured for PPP encapsulation.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCee94020

  Symptoms: The **timer** command to configure SPF and LSA may not be available.

  Conditions: This symptom is observed when the OSPF VRF process is configured.

  Workaround: There is no workaround.

- CSCef21601

  Symptoms: Calls may not complete because ResvConfirm messages are dropped. You can enter the **debug ip rsvp messages** command to track RSVP messages as they traverse routers.

  Conditions: This symptom is observed when RSVP is configured for call admission control in a network with routers that do not have RSVP and a proxy ARP enabled. The symptom occurs because the RSVP-capable hop that sends the ResvConfirm messages uses the next RSVP-capable hop as the next IP hop for the packets and does not have the MAC address that is needed to encapsulate the IP packets for this next IP hop.

  Workaround: Configure a static ARP entry that enables the router to properly encapsulate the packet by entering the **arp** *ip-address hardware-address* **arpa** command. The *ip-address* argument is the address of the next hop (that is visible via the RSVP debugs) for the ResvConfirm messages and the *hardware-address* argument is the MAC address of the interface of the next IP hop through which the ResvConfirm messages should be routed.

- CSCef86518

  Symptoms: A router may generate a series of error messages similar to the following and eventually pauses indefinitely because of a software-forced crash:

  ```
  %SYS-3-CPUHOG: Task is running for (2003)msecs, more than (2000)msecs (2/1),process
  = HSRP (Standby).
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for secure NAT (SNAT), NAT Stateful Failover, and HSRP.

  Workaround: Disable NAT Stateful Failover.

  Further Problem Description: In order for SNAT, NAT Stateful Failover, and HSRP to function together, enter the following commands:

  - Enter the **protocol udp** as part of the SNAT configuration.
  - Enter the **standby delay minimum** *min-delay* **reload** *reload-delay* for the SNAT-tied HSRP group.
  - Enter the **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] command for the SNAT-tied HSRP group.

- CSCeg07725

  Symptoms: A router may continue to redistribute an eBGP route into EIGRP after the eBGP route is deleted or EIGRP may not redistribute an eBGP route after the eBGP route has been installed.

  Conditions: This symptom is observed on a Cisco router that redistributes eBGP routes into EIGRP when the router functions in a multihoming environment.

  The symptom occurs in a configuration with two PE routers that advertise routes via eBGP and a border router that is configured with a higher local preference than the PE routers when the eBGP route of the primary path is withdrawn and the route of the secondary path is installed.

  Workaround: If a route is still redistributed into EIGRP after the eBGP route is deleted, clear the BGP peer from which the eBGP route used to be learned so EIGRP stops advertising the route.

  If a route is not redistributed into EIGRP after an eBGP route is installed, clear the route so EIGRP starts advertising it. Another workaround is to enter the **bgp redistribute-internal** command to cause EIGRP to redistribute iBGP routes and to prevent EIGRP from failing to redistribute an updated BGP route.

- CSCeg51291

  Symptoms: A VRF ping fails to reach an OSPF neighbor interface.

  Conditions: This symptom is observed when the platform on which the ping originates and the OSPF neighbor interface are connected via an OSPF sham link that is used for interconnecting traffic between two VPN sites.

  Workaround: There is no workaround.

- CSCeg58039

  Symptoms: Border Gateway Protocol (BGP) may crash.

  Conditions: This symptom is observed when the *number* argument of the **maximum-paths** *number* command is modified.

  Workaround: There is no workaround.

- CSCeg89700

  Symptoms: A Cisco router does not recognize an end-of-RIB message from a third-party vendor router and continues to show the “Neighbor is currently in NSF mode” message although the restart procedure of the third-party vendor router is complete.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 BGP peering and NSF. Note that the symptom does not occur when IPv4 BGP peering is configured.

  Workaround: There is no workaround.

- CSCeh07809

  Symptoms: When BGP nexthop information for a prefix changes because of topology changes, BGP properly updates its path information and IP routing table entry but CEF may not update the corresponding CEF entry, causing a stale entry. This inconsistency between BGP and CEF may cause a connectivity problem.

  Conditions: This symptom is observed when the nexthop information changes to an existing prefix entry in the BGP routing table. Typically, this occurs when the interface through which the prefix is learned goes down.

  Workaround: Flush out the stale CEF entry by entering the **clear ip bgp** command or withdraw and readvertise the prefix by the source router, which enables the affected router to refresh the CEF entry.

- CSCeh16989

  Symptoms: The Multiprotocol BGP (MP-BGP) network entries counter increases above the real number of reachable networks.

  Conditions: This symptom is observed when network activity occurs in a non-converged environment. The correct number of network entries is restored when there is a period of BGP stability that last for about 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is a sustained period of churn and BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the real number of reachable networks.

  Workaround: There is no workaround.

- CSCeh33504

  Symptoms: A router terminates 102,000 VPNv4 routes but route reflectors (RRs) report only a a subset of the total.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 when 204 routes are configured per VRF over 496 VPNs (one VPN has about 1000 routes). However, Cisco MGX RPM-PRs that function as RRs show that only 76245 routes are terminated on the Cisco MGX RPM-XF. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCeh35246

  Symptoms: A router may crash when a subinterface on which OSPF is running is deleted.

  Conditions This symptom is observed when the **mpls ldp sync** command is configured under OSPF.

  Workaround: There is no workaround.

- CSCeh37200

  Symptoms: A router crashes when PIM is enabled on a VIF interface.

  Conditions: This symptom is observed on a Cisco 7500 series but may be platform-independent.

  Workaround: There is no workaround.

- CSCeh47172

  Symptoms: Deny statements for an expanded list in the **ip extcommunity-list** command are ignored. Both named and numbered expanded extended community access lists are impacted.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 but is platform-independent.

  Workaround: Configure a route map, split complex extended community access lists in different simpler extended community access lists, and use permit statements and deny route-map statements.

- CSCeh47763

  Symptoms: A Cisco router may erroneously send ACK packets in response to RST packets for non-local TCP sessions. This can cause high CPU utilization on the router.

  Conditions: This symptom occurs when using Port Address Translation (PAT).

  Workaround: Use the **clear ip nat translation *** command.

- CSCeh49504

  Symptoms: BGP redistribution into EIGRP based on a standard community or AS path does not work as expected.

Conditions: This symptom is observed when the **match community** or **match as-path** route-map commands are enabled.

Workaround: There are two steps to this workaround:

1. Apply an inbound route map on the BGP neighbor. The inbound route map must include the **set metric** command to set the BGP multi-exit discriminator (MED) based on the standard community or AS path.
2. Match on the BGP MED in the route map that is used in the BGP redistribution.

Further Problem Description: Set actions in one particular statement that includes the **match community** or **match as-path** command are applied to all routes that match any subsequent statement in the same route map, instead of only to the routes that match the particular statement to which the set actions were applied.

- CSCei01284

  Symptoms: Internal IP routes may not be withdrawn, which may be verified in the output of the **show ip route summary** command.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP after you have shut down the loopback interface.

  Workaround: There is no workaround.

- CSCei08233

  Symptoms: A router that is configured for NAT may crash because of a bus error.

  Conditions: This symptom is observed when you enter the **clear ip nat translation *** command to clear all IP NAT translations or when NAT entries are deleted because they age out.

  Workaround: There is no workaround.

- CSCei26899

  Symptoms: When you reset a BGP peer, some prefixes are missing.

  Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- CSCei27084

  Symptoms: Configured NAT pools are not shown in the startup configuration and are not visible through CLI commands.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when you configure NAT pools after you have first configured a discontiguous NAT pool.

  Workaround: If you need only a single discontiguous NAT pool, configure it after you have configured other NAT pools.

- CSCin65241

  Symptoms: IS-IS redistribute commands are not synchronized to the standby RP. The routes that depend on these commands fail after a switchover.

  Conditions: This symptom is observed on a Cisco 7500 series but is platform-independent.

  Workaround: There is no workaround.

- CSCsa54937

  Symptoms: An LNS with a VRF configuration does not send an echo reply when it receives a ping to loopback interface 0.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-300, a Cisco 7200 series that is configured with an NPE-400, and a Cisco 7400 series.

  Workaround: Wait about 20 minutes to enable the LNS to send an echo reply or enter the **clear arp-cache** command.

- CSCsa55482

  Symptoms: A duplicate PIM register encapsulation tunnels may be created for a static rendezvous point.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 multicast when you configure a static rendezvous point after having disabled an embedded rendezvous point.

  Workaround: Configure the static rendezvous points while the embedded rendezvous point is enabled and then disable the embedded rendezvous point.

- CSCsa57101

  Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

  Conditions: The symptom is platform- and release-independent.

  Workaround: Disable SNMP by entering the **no snmp-server host** command.

- CSCsa63317

  Symptoms: A router may crash when both NAT and he Cisco Optimized Edge Routing (OER) feature are configured on the same router.

  Conditions: This symptom is observed on a Cisco router when a VRF instance is created and deleted via the OER feature.

  Workaround: There is no workaround. Do not combine NAT and the OER feature on the same router.

- CSCsa65155

  Symptoms: IS-IS may not update redistributed BGP network changes.

  Conditions: This symptom is observed when the **network** *network-number* command is enabled to introduce connected networks into a BGP topology and when, afterwards, BGP is redistributed into IS-IS. The symptom occurs after one of the interfaces that forms a network connection goes down and comes up again; the network re-enters the BGP topology but is no longer redistributed into IS-IS.

  Workaround: There is no workaround.

- CSCsa75512

  Symptoms: A crash that is related to OSPF flooding may occur on a Cisco router that is configured for OSPF and MPLS traffic engineering.

  Conditions: This symptom is observed when 1600 OSPF interfaces are configured in an OSPF area that is also configured for MPLS traffic engineering and when OSPF interfaces and OSPF adjacencies flap. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef16096. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: Reduce the number of OSPF interfaces in the OSPF area to 300 or less. You can check the number of OSPF interfaces by entering the **show ip ospf** or **show ip ospf interface** *interface-type interface-number* **brief** command. Note that all interfaces that are covered by network statements are counted.

- CSCsa80861

  Symptoms: Routes may not be properly removed when a route that is learned via Border Gateway Protocol (BGP) is withdrawn. This situation may cause an inconsistency in the control plane and may result in forwarding loops in the data plane.

  Conditions: This symptom is observed on a Cisco router when BGP is configured for route redistribution into an Interior Gateway Protocol (IGP) such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing (EIGRP).

  Workaround: There is no workaround.

- CSCsa87473

  Symptoms: A BGP speaker may fail to send all of its prefixes to a neighbor if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation causes the neighbor to miss some prefixes from its BGP table.

  Conditions: This symptom may occur between any pair of BGP speakers.

  A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). In this configuration, the symptom occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE.

  Workaround: There is no workaround.

- CSCsa94774

  Symptoms: When you enter the **traceroute** command from an IP address that is different from the address in the NAT default configuration, the incoming PAT sends the reply packets to the NAT default address that is defined in the NAT default configuration and not to the original source address from which the **traceroute** command was entered. Note that the outside PAT works fine.

  Conditions: This symptom is platform-independent. NAT overload traffic and other TCP traffic is not affected.

  Workaround: There is no workaround.

- CSCsa98059

  Symptoms: Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers that redistribute BGP into OSPF.

  Conditions: These symptoms are observed when at least two border routers are connected via eBGP to another autonomous system, receive the same prefix over these connections, and redistribute the prefix into OSPF. Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer flaps, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers.

  Workaround: There is no workaround.

- CSCsb07372

  Symptoms: NAT H.323 does not create an entry in the NAT translation table even though debugging shows that NAT processes the packet correctly. This situation causes one-way voice for the called party, preventing them from hearing the calling party.

  Conditions: This symptom is observed only when ICMP error messages are processed by NAT.

  Workaround: There is no workaround.

- CSCsb07649

  Symptoms: When UDP packets enter from the outside of a network to the inside of a network, new extended entries are created with an incorrect inside global port number in the translation entry. (Note that inside local port numbers are allocated correctly.) For each transferred NATted packet, one new entry is created with an incremented inside global port number. After the port pool has become exhausted, new extendable entries can no longer be created, preventing packets form being translated via NAT.

  Conditions: This symptom is observed on a Cisco router that has the **ip nat inside source static udp** *local-ip local-port global-ip global-port* **extendable** command enabled. The symptom may occur for all UDP ports that are assigned as system ports.

  The symptom does not occur for packets that pass from the inside of the network to the outside of the network, nor for TCP packets.

  Temporary Workaround: Reload the router to release the incorrectly allocated ports. This is a temporary workaround because the port pool will become exhausted again.

- CSCsb09709

  Symptoms: A router crashes because of a watchdog timeout when you remove a BGP configuration with an IPv6 Address Family Identifier (AFI).

  Conditions: This symptom is observed when you enter the **no router bgp** command for a BGP configuration with an IPv6 AFI.

  Workaround: There is no workaround.

- CSCsb34946

  Symptoms: When you add a second redundancy group, a router reloads and generates a traceback.

  Conditions: This symptom is observed on a Cisco router that is configured for HSRP and that has Stateful NAT configured and bound to the HSRP group.

  Workaround: There is no workaround.

- CSCsb35522

  Symptoms: Routers that are configured for Stateful NAT do not register each other when they are associated with an HSRP group that is configured on a VRF-aware interface.

  Conditions: This symptom is observed when the following conditions are present:

  - Redundant Cisco routers are connected to LAN segments.
  - The connectivity to the LAN is based on physical interfaces and a trunk.
  - Each interface/subinterface is assigned to a unique VRF.
  - Stateful NAT is configured to share the translation table between the active and standby translators.

  Workaround: Map the IDs of the various VRFs that are associated with the HSRP group. However, this workaround has the limitation that one interface has to be spared on the LAN. This situation could be a constraint if the network is configured in such a way that all interfaces have VRF enabled.

- CSCsb37698

  Symptoms: When you configure NAT, an IPv6 configuration is evoked unintentionally in addition to the NAT configuration.

  Conditions: This symptom is observed when you enter the **ip nat pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command. When you do so, the output of the **show running-config** command shows the above-mentioned command and, in addition and unexpectedly, also the **ipv6 nat v6v4 pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command.

  Workaround: There is no workaround.

- CSCuk56758

  Symptoms: BGP may crash in the bgp_clns_update_fwdtable_walker function.

  Conditions: This symptom is observed on a Cisco platform when the CLNS address family is used in BGP.

  Workaround: There is no workaround.

- CSCuk56949

  Symptoms: An MLD configuration is not copied from the startup configuration to the running configuration during the boot process, and the following error message is generated:

  ```
  %Error: MLD process could not be started
  ```

  Conditions: This symptom is observed when you boot a Cisco router with an existing configuration that contains MLD commands.

  Workaround: Reconfigure the MLD configuration after the router has booted.

ISO CLNS

- CSCeh00090

  Symptoms: Routes may be unexpectedly removed from the routing table.

  Conditions: This symptom is observed when IS-IS is used to advertise IP prefixes and when you enter a **distance** command that changes the overall configuration but keeps a subset of the prefixes at the same distance as in the previous configuration. The routes for which the distance does not change may be removed from the routing table.

  The following two examples show configurations in which the symptom occurs. When the distance configuration for IS-IS is **115 ip** and you enter one of the following command sequences, the symptom occurs:

  ```
  router isis
   distance 255 ip
   distance 115 ip
  ```

  or

  ```
  router isis
   distance 115 0.0.0.0 255.255.255.255
  ```

  Workaround: For all prefixes, configure distances that differ from the distances that were initially configured.

- CSCeh41328

  Symptoms: IPv6 routes that are learned from other IPv6 routers are not installed in the RIB.

Conditions: This symptom is observed on a Cisco router that is configured for Multi-topology IS-IS in transition mode. This symptom does not occur when the router is configured for Multi-topology IS-IS without the transition mode.

Workaround: Use the default IS-IS metric on the interfaces that are configured for IPv6 IS-IS.

- CSCsa61872

  Symptoms: IS-IS routes disappear unexpectedly from the routing table.

  Conditions: This symptom is observed when IS-IS is enabled on Gigabit Ethernet interfaces and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Gigabit Ethernet interfaces. When the symptom occurs, the IS-IS adjacencies are still up.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the same interface for a second time.

- CSCsa82134

  Symptoms: A router that is configured for IS-IS may reload unexpectedly.

  Conditions: This symptom is observe on a Cisco router when there are more than 64 equal-cost next hops for an IPv6 route that is learned from IS-IS.

  Workaround: There is no workaround. However, the conditions are unlikely to occur in a production network.

Miscellaneous

- CSCdy88212

  Symptoms: When you enter the **no match ip address** *access-list-number access-list-name...* route-map configuration command on a line card, the command is not removed and remains active, preventing Policy Based Routing (PBR) from being updated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2, 12.3, or 12.4.

  Workaround: There is no workaround.

- CSCdz67845

  Symptoms: The “Other counts” field in the output of the **show ip mroute** command is not accurate.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 or an earlier release.

  Workaround: There is no workaround.

- CSCed21063

  Symptoms: On a headend of an MPLS TE tunnel, a tag may be changed to an implicit null label when a RESV message is received with a different label than the one that was previously programmed. On the midpoint of the MPLS TE tunnel, the label is deprogrammed altogether for several seconds (15 to 30 seconds), causing a label mismatch to occur between the headend and the midpoint and packets to be lost.

  Conditions: This symptom is observed when a non-cisco P router changes the label on a TE tunnel without issuing a tear message. This situation causes a Cisco router to receive a RESV message with a different label than the one that was previously programmed and causes the Cisco router to program an implicit null label for the IP address that is associated with the tunnel.

Workaround: To restore proper traffic flowing, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected tunnel interface.

- CSCed43120

  Symptoms: Traffic rate distribution between classes during congestion is not according to the specified class bandwidth.

  Conditions: In RPM-XF platform, SAR-based QoS is used, output service policy is enabled with WRED configured and congestion is introduced in the VC.

  Workaround: Configure minimum and maximum thresholds for WRED as cells instead of as packets for SAR-based QoS although the CLI specifies it as packets.

- CSCed80272

  Symptoms: If two Cisco Multiservice IP-to-IP Gateways (IPIPGWs) are selected in the voice call path and both IPIPGWs are registered to the same gatekeeper, the second IPIPGW is not selected by the gatekeeper.

  Conditions: This symptom is observed when the IPIPGWs and endpoints are registered to the same gatekeeper.

  Workaround: Configure the IPIPGWs to register to the respective endpoint zones by entering the **zone local** *gatekeeper-name domain-name* **invia** *inbound gatekeeper* **outvia** outbound gatekeeper **enable-intrazone** command and configure prefixes for the endpoints on the gatekeeper.

- CSCee17241

  Symptoms: When the redundancy mode is changed from classic-split to RPR-plus through the command line interface (CLI), the peer Route Switch Controller (RSC) goes to the initial configuration setup dialogue.

  Conditions: This symptom has been observed on a Cisco AS5850 universal gateway.

  Workaround: Load the configurations with RPR-plus configured onto the startup configurations of both RSCs. The symptom will not be seen.

- CSCee28332

  Symptoms: MLP may fail or may be rejected on a PE router.

  Conditions: The symptom is observed on a Cisco 7500 series that functions as a PE router after a connected CE router is reloaded with a different Cisco IOS software image that it ran before.

  Workaround: Create a new multilink interface on the PE router or reload the VIP for the bundled physical interface on the PE router.

- CSCee32427

  Symptom: A Cisco 2691 may hang after crashing with the following error message:

  ```
  %ERR-1-GT64120 (PCI-0): Fatal error, DMA out of range error
  ```

  Conditions: This symptom is observed when you boot the Cisco 2691.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is only observed on a Cisco 2691.

- 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.

- CSCee42932

  Symptoms: Resuming a call that was placed on hold fails on a Cisco CallManager.

  Conditions: This symptom is observed when a Cisco CallManager that runs version 4.0 and that is not configured for Message Transport Protocol (MTP) is connected via an IPIPGW to another Cisco CallManager that runs version 4.0 and that is not configured for MTP.

  The symptom occurs on the second Cisco CallManager because the IPIPGW sends an incorrect ICT version for the first Cisco CallManager to the second Cisco CallManager and because the IPIPGW drops the non-standard fields in the callproc, alert, and connect messages from the second Cisco CallManager to the first Cisco CallManager.

  Workaround: Configure MTP.

- CSCee54143

  Symptoms: An E1 port on a PA-MC-8T1 port adapter may stay down after a VIP crash.

  Conditions: This symptom is observed on a Cisco 7513 that is configured with a VIP in which a PA-MC-8T1 port adapter with a channelized E1 (or T1) port is installed in slot 0.

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

- CSCee79728

  Symptoms: A Cisco 7200 series that operates in the process switching path may crash with a bus error exception.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(13b)M2 and that is configured with a serial or POS port adapter. The symptom may also occur in other releases.

  Workaround: Enter the **ip route cache** command for all interfaces.

- CSCee89537

  Symptoms: NBAR classification fails for GRE output packets.

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series that run Cisco IOS Release 12.3(8)T, that are configured for IPSec in GRE tunnel mode, and that have the **ip nbar protocol-discovery** command enabled. The symptom may also occur in other releases.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs both with software and hardware encryption.

- CSCef07167

  Symptoms: A VIP may crash and generate tracebacks when you perform and OIR of the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dLFI and MPLS VPN.

  Workaround: There is no workaround.

- CSCef07711

  Symptoms: A Cisco MGX-RPM-PR crashes with a crashinfo file indicating that it failed to reset the ATMizer (SAR) chip.

  Conditions: This symptom is observed when on a Cisco MGX 8850 in which an MGX-RPM-PR-512 is installed that runs Cisco IOS Release 12.2(15)T4e.

  Workaround: There is no workaround.

- CSCef08173

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

  Conditions: Problem gets 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.

- CSCef25686

  Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

  ```
  %ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface ATM
  X/X/X,
  (Cause of the failure: PVC removal during recreation failed)
  ```

  Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface** *interface-number* command.

  The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface** *interface-number* command via another Telnet (or console) session.

  Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCef44786

  Symptoms: ATM BADVCD error messages are generated and some packet or cell loss is associated with these messages. The cell loss can be observed as MLP fragment loss at the remote end by entering the **show ppp multilink** command.

  Conditions: This symptom is observed on a PA-A3 port adapter that is installed in a FlexWan on a Cisco Catalyst 6500 series that runs a Cisco IOS native software image when MLP over ATM is configured with dLFI on the PA-A3. The symptom occurs only when QoS is configured for dLFIoATM and when the last fragment size is slightly smaller than the number of fragments multiplied by the VC encapsulation size.

  Workaround: You can reduce the chances that the symptom occurs by configure a larger delay, which diminishes the number of fragments.

  Alternate Workaround: If this an option, configure the PVC at 192 kbps or a higher bandwidth, which also ensures large fragment sizes.

- CSCef48325

  Symptoms: WRED counters do not function on distributed platforms such as a Cisco 7500 series and a Cisco 7600 series.

  Conditions: This symptom is observed on a distributed Cisco platform that runs Cisco IOS Release 12.0(26)S3, 12.0(29)S, 12.2(25)S, 12.3(10), or 12.3(11)T and that has dWRED configured.

  Workaround: There is no workaround.

- CSCef72129

  Symptoms: When a router is configured for create on-demand VCs and PPPoA sessions, the CPU use of the RP may become extremely high when VCs and sessions are brought up and torn down.

  Conditions: This symptom is observed only when the configuration contains around 30,000 PPPoA sessions and when additional services such as DBS, ACLs, and service policies are enabled.

  Workaround: Lower the amount of PVS statements on a single subinterface to reduce the CPU use of the RP.

- CSCef72756

  Symptoms: A Cisco IP phone may not have access to network resources because it cannot perform TTP-, FTP-, or Telnet-based authentication.

  Conditions: This symptom is observed on a Cisco IP phone that is connected behind a Cisco router on a interface that is configured for Authentication Proxy.

  Workaround: Add the Cisco IP phone source IP address as a “deny entry” in the Authentication Proxy Intercept ACL so that IP phone is bypassed for authentication, and ensure that the interface ACL has a permit statement for the IP phone.

- CSCef82962

  Symptoms: A call treatment only plays a busy tone instead of the audio file that is configured in the call treatment.

  Conditions: This symptom is observed when call treatment is configured on a router that functions as a Cisco CallManager Express (CME) and when the call threshold is met.

  Workaround: There is no workaround.

- CSCeg05925

  Symptoms: After you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a VLAN interface, MPLS traffic is dropped.

  Conditions: This symptom is observed only when MPLS static labels are configured. When an MPLS TFIB entry is created using MPLS static labels and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the egress VLAN interface, the MPLS entry may be missing from the TFIB on the line cards or port adapters.

  Workaround: Enter the **clear ip route** command for the affected prefix.

- CSCeg14231

  Symptoms: Various commands that include the **virtual access** keywords do not work as expected. For example, the **show policy-map interface virtual-access2.1** produces no output even when there is policy map data associated with interface virtual-access2.1.

  Conditions: This symptom is observed only on certain commands and only when these commands specify a virtual access interface.

  Workaround: There is no workaround. However, the symptom is not service-affecting.

- CSCeg15065

  Symptoms: After a DSP restarts, RTP packets are not sent from the DSP to a trunk connection.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that runs Cisco IOS Release 12.3(10a) or Release 12.3(11)T when the **connection trunk** command is enabled.

Workaround: There is no workaround. To re-enable the DSP to send RTP packets, enter the enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the voice port that is associated with the DSP.

- CSCeg16631

  Symptoms: When you enter the **distribute-list** *interface* command in a global RIP routing context and the interface that is specified in the command is a VRF interface, the command is rejected with the following error message:

  ```
  % The interface is not in the same VRF as the process
  ```

  Because the **distribute-list** *interface* command is not implemented in the IPv4 VRF address-family, there is no other way to filter networks received in updates via a VRF interface.

  Conditions: This symptom is observed in all Cisco IOS releases that integrate the fix for CSCee32557. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee32557. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: In a configuration that is mentioned above, to filter networks received in updates, enter the **distribute-list** *extended-ACL-reference* command in which the "source-part" of the extended ACL specifies the prefixes and the "destination part" matches on the IP address of the RIP neighbor.

- CSCeg17082

  Symptoms: All voice calls fail and the output of the **show voice port summary** command shows that all voice ports are in the down state:

  ```
  IN       OUT
  PORT      CH   SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
  ========= == ============ ===== ==== ======== ======== ==
  0/1:0     01  e&m-wnk     up    down idle     idle     y
  0/1:1     02  e&m-wnk     up    down idle     idle     y
  0/1:2     03  e&m-wnk     up    down idle     idle     y
  ```

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3660, and Cisco 3700 series that run Cisco IOS Release 12.3(11)T1 or Release 12.3(11)T2 and that are configured with an AIM-VOICE interface module that has DSPs that are configured for high complexity. The symptom occurs after you reload the router.

  Workaround for Release 12.3(11)T1: Bring the voice ports to the up state by entering the **shutdown** voice-port configuration command followed by the **no shutdown** voice-port configuration command on the affected voice ports.

  Workaround for Release 12.3(11)T2: Remove the affected DS0 group and reconfigure it.

- CSCeg24422

  Symptoms: Packet drops occur in the ingress direction on a dMLP or dMLFR link with traffic at 95-percent of the line rate and when the number of packets with a small size is high.

  Conditions: This symptom is observed on a Cisco 7500 series that functions as a provider edge (PE) router, that is configured for L2TPv3 L3VPN, and that has dMLP or dMLFR links to a customer edge (CE) router.

  Workaround: There is no workaround.

- CSCeg24938

  Symptoms: A Cisco RPM-XF resets when you enter the **clear ip mroute *** command repeatedly.

  Conditions: This symptom is observed when the Cisco RPM-XF is configured for low speed.

Workaround: There is no workaround.

- CSCeg26528

  Symptoms: The performance of a router may be severely degraded (at approximately 90 percent of the line rate) when large packets are processed, when the MLP bundle link flaps, and when the router does not recover the MLP sequence numbers of the packets.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured for dMLP only when large packets are processed.

  Workaround: There is no workaround.

- CSCeg27984

  Symptoms: A modem that is connected to a Cisco 830 series is not recognized properly and the settings in the line configurations are not recognized properly.

  Conditions: This symptom is observed when the modem is connected while you reload the Cisco 830 series.

  Workaround: There is no workaround.

- CSCeg31293

  Symptoms: Interfaces change to the down/down state and are unable to pass traffic because interprocess communications (IPC) fails between a line card and the RP.

  Conditions: This symptom is observed when a line card of a Cisco 10000 series is removed and inserted via an OIR. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeg32948

  Symptoms: A ping from a home agent (HA) to a mobile access router (MR) fails with CEF is enabled on the foreign agent (FA).

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when the MR or the mobile node (MN) roams to another interface on the same FA.

  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.

- CSCeg39560

  Symptoms: After a router is rebooted, a tunnel interface does not acquire the IP address of the async serial interface that is the tunnel source.

  Conditions: This symptom is observed on a Cisco 2600 series that runs Cisco IOS Release 12.3(8)T3.

  Workaround: Enter the **tunnel source interface-type** *interface-number* command on the tunnel interface.

- CSCeg40721

  Symptoms: Tail drops occur on SAR CoS queues that are configured on a Cisco MGX 8800 series RPM-XF that is configured for low speed (also referred to as an RPM-XFL) and that functions as a PE router.

Conditions: This symptom is observed when SAR-based QoS is configured and bursty traffic is sent on VCs that do not have output policy maps configured.

Workaround: Depending on the size of the bursts, increasing the queue size may help to absorb the bursts. However, doing so may increase the delay and, if the queue size is increased on many VCs, may significantly increase the buffer use.

- CSCeg43855

  Symptoms: An encrypting router may send traffic that is locally originated (such as keepalive packets or routing update packets) out of order after the packets have been encrypted. Because of the anti-replay check failure, these packets are dropped on the receiving router.

  Conditions: This symptom is observed when a multipoint GRE (mGRE) and IPSec tunnel is build between two routers.

  Workaround: Turn off packet authentication for the configured IPSec transform.

  Further Problem Description: On a Cisco 7200 series that functions as the receiving router, you can observe the symptom in the output of the **show crypto ipsec sa detail** or **show pas isa interface** command.

- CSCeg53478

  Symptoms: A Cisco 831 may display the following message on the console:

  ```
  pktFlowLink() logic error, pMatch and pEmptySlot
  ```

  Conditions: This symptom is observed very rarely after the router has been up for a long time. The functionalities of the router are not affected.

  Workaround: There is no workaround.

- CSCeg57219

  Symptoms: You cannot ping with packets of certain sizes after an RPR+ switchover or after an interface flap on a multilink interface that has members of non-channelized port adapters when the multilink interface is configured with fragmentation and interleaving.

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCeg58427

  Symptoms: When multicast packets are dropped because of PXF programming errors, you can not easily detect these errors on input interfaces that are part of the Multicast Forwarding Information Base (MFIB).

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-XF that is configured for PXF forwarding.

  Workaround: Compare the output of the **show pxf cpu mroute** command and **show ip mroute** commands and check for any inconsistencies in the input interface information.

- 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 7500 series that runs Cisco IOS Release 12.2S or Release 12.3 and that is configured with a PA-MC-8TE1+ port adapter.

  Workaround: There is no workaround.

- CSCeg70465

  Symptoms: There is no QoS classification at a main interface when packets are switched from a GRE tunnel that also has a QoS policy enabled.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3T or Release 12.4 when a QoS policy is enabled on both the GRE tunnel and the main interface in the output direction.

  Workaround: Move the complete QoS configuration to the QoS policy on the main interface (that is, use an hierarchical policy).

- CSCeg72989

  Symptoms: IPv6 static neighbors that are configured over a Gigabit Ethernet WAN (GE-WAN) interface may not appear in the IPv6 neighbor table.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series after the platform is reloaded and the GE-WAN interface is up. The symptom may be platform-independent and may also occur with other Gigabit Ethernet interfaces.

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

- CSCeg74562

  Symptoms: A router may take a very long time to establish LDP sessions with its peers and advertise its label bindings. In some cases, the LDP sessions may flap.

  Conditions: This symptom may occur when a Cisco router that uses LDP for label distribution has a large number (greater than 250) of LDP neighbors and several thousand label bindings to advertise.

  Workaround: The time required to establish the neighbor sessions and advertise the label bindings when TDP is used in place of LDP may be substantially less. Using TDP in place of LDP will result in an acceptable convergence behavior.

- CSCeg74772

  Symptoms: When you enter the **clear cef linecard** command, IDBs may be hold on the line card. When you enter the **clear cef linecard** command, the number of IDBs that are used on the line card increases.

  Conditions: This symptom is observed on a Cisco platform when a GRE tunnel interface is used.

  Workaround: There is no workaround.

  Further Problem Description: When many tunnel interfaces are used and when the **clear cef linecard** command is entered several times, the SWIDB number may reach its upper limit. If this situation occurs, you must reload the platform.

- CSCeg75974

  Symptoms: A router sends a SSG Prepaid authorization requests to the AAA server instead of to the SSG Prepaid server.

  Conditions: This symptom is observed on a Cisco router that is configured for SSG RADIUS Proxy and SSG Prepaid, that uses the PZS attribute in the local SSG service profile, and that has been up and running for several weeks.

  Workaround: Do not configure the SSG Prepaid server via the PZS attribute in the local SSG Service profile but manually configure the SSP Prepaid server by entering the following commands:

  aaa group server radius *server-group-name* **server** *ip-address* **auth-port** *auth-port* **acct-port** *acct-port*
  ssg aaa group prepaid *server-group-name*

- CSCeg78036

  Symptoms: The following tracebacks may be generated when VFR handles fragmented packets:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 6472EE80
  chunkmagic 0 chunk_freemagic 6484FA7C
  -Process= "IP Input", ipl= 4, pid= 60
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.3(12.11)T1 and that is configured with a virtual reassembly. The symptom may also occur on a Cisco 2651XM.

  Workaround: Disable the virtual reassembly by entering the **no ip virtual-reassembly** command.

- CSCeg80436

  Symptoms: When you enter the **no mgcp** command followed by the **mgcp** command (that is, you restart the MGCP process), the ports that are configured for PRI backhaul enter the "not ready" state, which is shown in the output of the **show mgcp end db** command.

  Conditions: This symptom is observed on a Cisco 3800 series.

  Workaround: There is no workaround.

- CSCeg80842

  Symptoms: The output of serial interfaces on a PA-MC-8TE1 may become stuck after several days of proper operation.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(10a) and that has MLP configured on the serial interfaces of the PA-MC-8TE1.

  Temporary Workaround: Perform an OIR of the PA-MC-8TE1 or reload the router until the symptom occurs again.

  Further Problem Description: The symptom occurs during normal operation of the router. If many errors occur on the link, the symptom is more likely to occur.

- CSCeg81454

  Symptoms: When you reload a Cisco 836 or a Cisco 837, a CPUHOG error may occur.

  Conditions: This symptom is observed on a Cisco 836 and Cisco 837 that have a minimal configuration and no traffic load.

  Workaround: Enter the **scheduler max-task-time 50000** command.

- CSCeg83460

  Symptoms: Bidirectional PIM DF election does not occur correctly when a PIM neighbor expires.

  Conditions: This symptom is observed when the PIM neighbor that expires is the designated forwarder (DF) for multiple RPs. The DF election is triggered only for the first RP on the list and does not occur for all the other RPs.

  Workaround: Clear the state of the DF or toggle the interface state of the DF.

- 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.

- 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.

- CSCeg87507

  Symptoms: DSP programming on a router fails, causing a BRI call to disconnect. The output of the **debug voip vtsp session** command shows “DSP programming failed”.

  Conditions This symptom is observed on a Cisco 2800 series, Cisco 3800 series, and any other router that uses Flex DSP resource management (DSPRM) when calls are made from a BRI or PRI to the PSTN and when the PSTN side sends a Call Proc message followed by a Call Alerting message.

  Workaround: There is no workaround.

- CSCeg87727

  Symptoms: Duplicate digits are generated for an incoming call.

  Conditions: This is observed on a Cisco IAD2430 that runs Cisco IOS Release 12.3(11) or Release 12.3(11)T2 when overlap is configured but DID is not.

  Workaround: Configure DID on the Cisco IAD2430.

- CSCeg88739

  Symptoms: Computer Assisted Law Enforcement Act (CALEA) support for call content may not function, that is, no duplicated call content may be generated.

  Conditions: This symptom is observed when CALEA support for call content is configured on a Cisco AS5400, when the target has call forwarding immediately activated, and when an off-net call is received that is forwarded back off-net (that is, the call is hairpinned) using the same Cisco AS5400. In this situation, no duplicated call content is sent to the mediation device. However, the MGCP “create connection” message from the associated BTS (which runs version 4.4) appears to be correctly formatted and successfully parsed by the Cisco AS5400.

  Note, however, that the symptom may occur for all call types, not just for hairpinned calls.

  Workaround: There is no workaround.

- CSCeg89017

  Symptoms: MGCP calls fail with a fast busy signal. When you enter the **debug mgcp packet** command, the output indicates that the 400 Voice Call Setup failed.

  Conditions: This symptom is observed when MGCP PRI backhaul is configured on a Cisco 2800 series that is configured with PVDM2 DSPs. Calls fail only after the router is reloaded. The symptom may also occur on a Cisco 3800 series that functions in the same configuration.

  Workaround: Enter the following sequence of commands:

  1. Enter the **ccm-manager config server** *ip-address* command followed by the **ccm-manager config** command.
  2. Enter the **shutdown** command on the voice port or on the T1 controller.
  3. Enter the **no mgcp** command followed by the **mgcp** command.

4. Enter the **no ccm-manager config** command followed by the **ccm-manager config** command, assuming that you have the TFTP server defined.
5. After you reload the router, enter the **write erase** command, add the configuration, and save the configuration.

- CSCeg89043

  Symptoms: A Cisco gateway may reload unexpectedly because of a SegV exception at address PC 0x80FF6340.

  Conditions: This symptom is observed when the gateway is configured for VoIP and fallback to an SNMP trap.

  Workaround: There is no workaround.

- CSCeh05517

  Symptoms: PXF programming errors in the output interface list of the multicast FIB are difficult to detect.

  Conditions: This symptom is observed on a Cisco 8800 MGX series RPM-XF that is configured for PXF forwarding when multicast forwarding is affected.

  Workaround: Compare the output of the **show pxf cpu mroute** and **show ip mroute** commands and check for any inconsistencies in the outgoing interface list information.

- CSCeh05968

  Symptoms: Distributed Sessions Manager (DSM) is flooded with DSP stats messages.

  Conditions: This symptom is observed when the event pool is out of events.

  Workaround: There is no workaround.

- CSCeh08689

  Symptoms: When CRTP is enabled on a PPP over Frame Relay PVC via a policy-map configuration, the service policy on the PVC does not function properly because packets are not placed in the priority queue. The output of the **show policy-map interface** command does not show a class counter.

  Conditions: This symptom is observed when you attach a policy map with CRTP on a virtual-template interface and then attach a policy map with a priority feature on the Frame relay PVC. Note that the symptom does not occur for a PPP over ATM PVC or PPP over Ethernet configuration.

  Workaround: There is no workaround.

- CSCeh10646

  Symptoms: A router may unexpectedly reloads because of a bus error at an address that falls just short of the I/O memory range such as address 0x4E7FD5B8, whereas the iomem address starts at 0x4E800000.

  Conditions: This symptom is observed when the router has some of the following security feature commands enabled on one or more interfaces:

  ```
  ip nbar protocol-discovery
  ip virtual-reassembly
  ip access-group in
  ip access-group out
  ip inspect in
  ip inspect out
  ```

```
ip ips in
ip ips out
auto discovery qos
crypto map
```

Workaround: Remove the **ip access-group out** command.

- CSCeh14272

  Symptoms: Prioritized encrypted traffic is dropped.

  Conditions: This symptom is observed when the Low Latency Queuing (LLQ) for IPSec Encryption Engines feature is enabled.

  Workaround: Disable QOS preclassification on the crypto map.

- CSCeh14446

  Symptoms: The maintenance mode on a Cisco AS5850 that is configured for RPR+ may not function.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(11)T but is release- and platform-independent.

  Workaround: There is no workaround.

- CSCeh15949

  Symptoms: An extended access list does not function when it is applied to an interface even though the access list is configured correctly.

  Conditions: This symptom is observed on a Cisco MGX 8850 RPM-XF that runs Cisco IOS Release 12.3(7)T3.

  Workaround: Use an external device to filter the traffic. Apply the filter at another location in the network to accommodate your needs. If this is not possible, call Cisco TAC and reference this caveat with DDTS ID CSCeh15949.

  Further Problem Description: An example of this caveat is shown below.

  When a router attempts to access the Fast Ethernet interface of the RPM-XF, the router is able to access the RPM-XF even though its Fast Ethernet interface has an access list applied to it.

  Topology:

```
RPM-XF-(FE)-------(FE)--Router
ip: 10.10.10.2      .1
```

```
Router_RPM09_XF#show running-config
Building configuration...
```

```
Current configuration : 1190 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_RPM09_XF
!
boot-start-marker
boot system x:rpmxf-p12-mz.123-7.T3
boot system bootflash:rpmxf-p12-mz.123-7.T3
boot-end-marker
```

```
interface FastEthernet2/0
ip address 10.10.10.2 255.255.255.252
ip access-group 101 in
duplex auto
speed auto

access-list 101 deny   tcp any host 10.10.10.2 eq telnet
access-list 101 permit ip any any

Router_RPM09_XF#show ip access-list 101

Extended IP access list 101 (Compiled)
10 deny tcp any host 10.10.10.2 eq telnet
20 permit ip any any (96 matches)
Router_RPM09_XF#
```

The information below shows that the access list does not function:

```
Router#telnet 10.10.10.2
Trying 10.10.10.2 ... Open
```

- CSCeh16214

  Symptoms: A router reloads when you connect a third-party USB card reader.

  Conditions: This symptom is observed when you connect a third-party USB card reader to the USB ports of a Cisco 2851 and Cisco 3845. It does not matter whether or not there is compact flash card in the USB card reader.

  Workaround: There is no workaround.

- CSCeh16887

  Symptoms: The unchannelized mode on a PA-MC-2T3+ port adapter does not function. The line protocol of an unchannelized interface remains down.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-2T3+ port adapter after you have entered the **no channelized** command.

  Workaround: There is no workaround.

- CSCeh17689

  Symptoms: Poor voice quality may be experienced as the default impedance selection may not yield the best ERL.

  Conditions: This symptom is observed on a Cisco 2800 series when you use the default impedance selection.

  Workaround: Enter the **test voice port** *slot subunit port* **inject-tone local sweep** *sweep step high amplitude low amplitude* command to manually calibrate the best ERL.

- 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.

- CSCeh17995

  Symptoms: When you enter the following commands on the Fast Ethernet port of an NM-16ESW network module, the router may crash:

  ```
  ip dhcp client hostname

  no switchport mode
  ```

`switchport mode`

Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series in which an NM-16ESW network module is installed.

Workaround: Do not enter IP commands in switchport mode.

- CSCeh18901

  Symptoms: When you insert an NM-2FE2W network module via an OIR, the terminal line number is increased by one. For example, if the there are 16 terminal lines before the OIR, there appear to be 17 terminal lines after the OIR.

  Conditions: This symptom is observed on a Cisco 3800 series. The symptom may also occur with an NM-16A network module or with an HWIC-16A WAN interface card.

  Workaround: Reload the router.

- CSCeh19106

  Symptoms: A Service Selection Gateway (SSG) that is deployed in a GPRS access environment and that is configured for L2TP tunnel service with an extended autodomain may reload when duplicate GPRS PDP context create requests are sent.

  Conditions: This symptom is observed when the PDP context create requests contain the static addressing, that is, the IP address of the MS instead of all zeros in the end user address field.

  Workaround: There is no workaround. Note that for corporate access through a GPRS access-based solution using SSG, generally dynamic addressing is used. With dynamic addressing, the end-user address field is sent with all zeros and the corporate network provides the address, and the symptom does not occur.

- CSCeh20048

  Symptoms: When you enter the **show crypto session** command, tracebacks and %SYS-3-BADLIST_DESTROY error messages may be generated.

  Conditions: This symptom is observed on a Cisco router that is configured for IPSec and multiple crypto tunnels.

  Workaround: There is no workaround.

- CSCeh21290

  Symptoms: When MLP is configured and when the policy map of a CE router does not have a real-time class map configured in its output policy map, TCP packets are policed incorrectly. This situation may affect the traffic throughput.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that functions as a PE router and that runs Cisco IOS Release 12.3(11)T3 or releases later than Release 12.3(2)T6. The symptom occurs when TCP packets are sent via class-b data with 73 bytes of payload from a CE router to a PE router.

  When the output policy map of the CE router does not have a real-time class map configured, the PE router shows that the 73-byte packet requires three ATM cells instead of just two ATM cells.

  When the output policy map of the CE router does have a real-time class map configured, the PE router shows that the 73-byte packet requires two ATM cells, as it should be.

  Workaround: There is no workaround.

- CSCeh21613

  Symptoms: When multicast is configured as part of a dial-peer configuration and you enter the **shutdown** command quickly followed by the **no shutdown** command on a voice port that is part of the dial-peer configuration, the router may generate tracebacks and may crash.

Conditions: This symptom is observed on a Cisco 1760 that runs Cisco IOS Release 12.3(11)T4.

Workaround: There is no workaround.

- CSCeh21680

  Symptoms: A Cisco 2800 series or Cisco 3800 series may crash when you configure the interface of an NM-16ESW.

  Conditions: This symptom is observed when you enter the **ip rsvp bandwidth** command on FE port 1/10 of the NM-16ESW and then you enter the **no switchport mode** command followed by the **switchport mode** command.

  Workaround: Do not enter IP commands in switchport mode.

- CSCeh22616

  Symptoms: The output queue of a Fast Ethernet back card of a Cisco MGX RPM-XF may be stuck at 40/40.

  Conditions: This symptom is observed when the Cisco MGX RPM-XF runs Cisco IOS Release 12.3(2)XZ and when the interface of the Fast Ethernet back card is configured in half-duplex mode and is connected to a hub. This symptom may also occur in Release 12.3T.

  Workaround: Clear the affected interface of the Fast Ethernet back card by entering the **clear interface fastethernet** *slot/port* command.

- CSCeh23047

  Symptoms: After a manual SSO switchover, traffic in the tag switching-to-IP switching direction between an egress 1-port 10-Gigabit Ethernet Engine 4+ line card and an ingress 4-port Gigabit Ethernet ISE line card does not recover.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S. However, the symptom is platform-independent and may also occur on other platforms that function in a similar configuration and that run other releases.

  Workaround: Reload microcode onto the 4-port Gigabit Ethernet ISE line card.

- CSCeh23742

  Symptoms: A DSP on a C549 Digital Signal Processing Module (DSPM) may time out on an originating gateway, on a terminating gateway, or on both, and the following error message may be generated:

  ```
  %DSMP-3-DSP_TIMEOUT: DSP timeout on DSP 0/14:2: event 0x0,
  S_DSMP_RSC_REOPENING
  Session information: session=0x64BAF558 dsp_intf=0x640C6F08 dsp_name=0/14:2
  ```

  Conditions: This symptom is observed on a Cisco 3640 that runs the c3640-is-mz image of Cisco IOS interim Release 12.4(0.4) and that is configured with a voice network module that contains a C549 DSPM when you first make a call via T.38 fax relay and then make a call via modem relay on a single DSP of a C549 DSPM.

  Workaround: First make the a call via modem relay, then make a call via T.38 fax relay.

- CSCeh24075

  Symptoms: Packets that are larger than 4400 bytes or packets that require fragmentation may be dropped when they traverses a xDSL WIC.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(6)T or a later release when a sweep ping is performed from one peer to another and when the WIC is a WIC-1ADSL, WIC-1ADSL-DG, WIC-1ADSL-I-DG, WIC-SHDSL, or WIC-SHDSL-V2.

Workaround: Avoid fragmentation on the DSL link or enter the **ip mtu** *bytes* command to change the maximum MTU to 4400 on the DSL interface.

- CSCeh24202

  Symptoms: A Cisco 2800 series that is configured for software or hardware encryption and CBAC may reload.

  Conditions: This symptom is observed when IPSec SAs and CBAC sessions are established and when the traffic is blocked by an ACL on the outgoing WAN interface of a neighboring crypto router. When you send encrypted traffic from the neighboring crypto router to another router via the Cisco 2800 series, the Cisco 2800 series reloads.

  Workaround: Permit the encrypted traffic on the outgoing interface of the neighboring crypto router.

- CSCeh24815

  Symptoms: High CPU utilization occurs on a Cisco AS5850.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(11)T3 when dCEF is not applied to packets because of a slow start configuration.

  Workaround: Remove the slow start configuration.

- CSCeh25036

  Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a switch subinterface, PPP is not re-established.

  Conditions: This symptom is observed on a Cisco 8800 MGX series RPM-XF.

  Workaround: Clear the virtual access interface that is associated with the switch subinterface.

- CSCeh25446

  Symptoms: The following error message may be generated when a Cisco AS5850 voice gateway boots:

  ```
  Could not enable MAC
  ```

  This situation may prevent line cards from booting up and pings over the Fast Ethernet and Gigabit Ethernet interfaces may fail.

  Conditions: This symptom is observed on a Cisco AS5850 voice gateway that runs Cisco IOS Release 12.3T.

  Workaround: There is no workaround.

- CSCeh25459

  Symptoms: A call fails when the codec is changed from G.729 to G.711ulaw during the call.

  Conditions: This symptom is observed when fax pass-through is configured and when the following events occur:

  – The initial codec for the call is negotiated as G.729.
  – A reinvite message with a codec change to G.711ulaw is sent to the gateway.
  – The gateway accepts the change with a 200 OK message but continues to send the call with codec G.729 in the RTP stream.

  Workaround: Remove the fax pass-through configuration.

- CSCeh27734

  Symptoms: For recursive routes with implicit null as the local label, the FIB may point to the rewrite of the parent prefix. However, this situation may not affect any functionality.

  Conditions: This symptom is observed on a router that is configured for MPLS forwarding.

Workaround: Change the affected prefix to be non-recursive.

- CSCeh27775

  Symptoms: While a USB flash drive or eToken is accessed, console access to a Cisco 1800 series, Cisco 2800 series, and Cisco 3800 series may be slow.

  Conditions: This condition is observed when a USB device is accessed with any file system command such as the **copy** command, **dir** command, or **format** command.

  Workaround: Power-cycle the router.

  Further Problem Description: The symptom occurs rarely and only impacts the speed of the console and the speed of USB device access. The router still processes other events as usual. The console is slow because it waits for the USB device access to complete. Once the USB device access is complete, any further USB device accesses are slow until the router is power-cycled. The USB device accesses do complete but may take several minutes to complete.

- CSCeh27783

  Symptoms: A router crashes after you have manually configured 237 IPv6 tunnels.

  Conditions: This symptom is observed on a Cisco platform that is configured for IPv6 when there are more than eight paths for one IPv6 prefix. The symptom is platform-independent and not release-specific.

  Workaround: There is no workaround.

- CSCeh27803

  This caveat consists of two (identical) symptoms, two conditions, and two workarounds:

  1. Symptom A: An MLP bundle is not set up completely on an RPM-XF, causing MLP traffic to be lost.

     Condition A: This symptom is observed when MLP peers use the same MLP endpoint discriminators.

     Workaround A: Configure unique endpoint discriminators on the peers. If identical endpoint discriminators must be used, configure an unique authentication for the peer.

  2. Symptom B: An MLP bundle is not set up completely on an RPM-XF, causing MLP traffic to be lost.

     Condition B: This symptom is observed when more than two links are forced to use the same MLP bundle.

     Workaround B: An RPM-XF supports MLP with LFI and is designed to support only one link per bundle. Reverify the configuration.

- CSCeh27915

  Symptoms: A Cisco 800 series RPM-PR resets unexpectedly, and a switchover occurs.

  Conditions: This symptom is observed when you enter the **no shutdown** interface configuration command on the interface of an MGX-RPM-1FE-CP back card.

  Workaround: Disable the **rpm hw-module fecp fc** command before you enter the **no shutdown** interface configuration command.

- CSCeh28320

  Symptoms: A Cisco 7600 series that has a FlexWAN, Enhanced FlexWan, or SIP-200 and that is configured for IP RTP compression in IPHC format may drop packets when RTP compression is disabled.

Conditions: The symptom is observed when RTP compression is disabled on an interface after an SSO switchover has occurred.

Workaround: Reload the router.

- CSCeh30146

  Symptoms: A WIC-1DSU-T1-V2 WAN interface card may become stuck and may not detect any alarms or loopback events but may still be able to pass traffic.

  Conditions: This symptom is platform-independent.

  Workaround: Enter the **clear service-module serial** *number* command.

- CSCeh30818

  Symptoms: A traceback is generated when multicast traffic is flowing.

  Conditions: This symptom is observed when PIM is enabled on multiple interfaces and when the counters are cleared.

  Workaround: There is no workaround.

- CSCeh30975

  Symptoms: The FXSLS voice port is stuck in an on-hook state, and the digital signal processor (DSP) is not released.

  Condition: This symptom occurs when the FXSLS user stays offhook at the end of the call after Cisco IOS software sends a Howler tone to the FXSLS port.

  Workaround: There is no workaround.

- CSCeh31306

  Symptoms: A Cisco MGX RPM-PR does not boot up.

  Conditions: This symptom is observed when the Cisco MGX RPM-PR does not receive the boot acknowledgement from the PXM.

  Workaround: There is no workaround.

- CSCeh31691

  Symptoms: Changing the encapsulation of a POS interface from HDLC to PPP or the other way around causes the link to go down.

  Conditions: This symptom is observed when you change the encapsulation of a POS interfaces on an Optical Services Module (OSM).

  Workaround: Power-cycle the OSM by entering the **no power enable module** *slot* command followed by the **power enable module** *slot* command.

- CSCeh32576

  Symptoms: Configuring an AUX port through a non-slotted notation such as “interface async 1” may not be possible on a Cisco 1841 and a Cisco 2801.

  Conditions: This symptom is observed on a Cisco 1841 and Cisco 2801 that run Cisco IOS interim Release 12.3(11.9)T or a later release.

  Workaround: Configure the AUX port through the slotted notation such as “interface async 0/0/0”.

- CSCeh33492

  Symptoms: A router may generate a %HAL-1-INITFAIL error message and may crash when you insert a PA-MC-STM-1MM port adapter via an OIR.

  Conditions: This symptom is observed on a Cisco 7200 series.

Workaround: There is no workaround.

- CSCeh33531

  Symptoms: A traceback is generated when you successfully insert a PA-MC-STM-1MM port adapter via an OIR.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: There is no workaround.

- CSCeh33913

  Symptoms: NAT-PT stops working after a router is reloaded.

  Conditions: This symptom is observed on a Cisco router that has a "v6v4" static NAT configuration when NAT-PT fails to install ARP entries because the router is not yet fully initialized.

  Workaround: Remove and then reconfigure the mapping.

- CSCeh34089

  Symptoms: You cannot run the Embedded Event Manager Tcl policy scripts.

  Conditions: This symptom is observed in all Cisco IOS software images that contain the fix for caveat CSCeg07394. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07394. 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.

- CSCeh35324

  Symptoms: Weighted Random Early Detection (WRED) does not match packets based on any marking done.

  Conditions: This symptom has been observed when qos pre-classification (the **qos pre-classify** command) is turned on.

  Workaround: Remove the **qos pre-classify** command.

- CSCeh35376

  Symptoms: Any type of call (voice, modem, or fax) that is made after a fax-relay call over the same connection trunk causes a DSP to crash.

  Conditions: This symptom is observed on a Cisco router that is configured for SIP. The symptom does not occur when the router is configured for H.323.

  Workaround: There is no workaround.

- CSCeh35411

  Symptoms: A line card or port adapter may crash repeatedly when the router in which the line card or port adapter is installed comes up after a software-forced crash has occurred on the router.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 MPLS and that has redundant RPs that are configured for SSO. The symptom is more likely to occur when the **ipv6 unicast-routing** command is enabled.

  Workaround: To diminish the chance that the symptom occurs, disable the **ipv6 unicast-routing** command.

- CSCeh35434

  Symptoms: An Embedded Event Manager TCL policy does not function.

Conditions: This symptom is observed on a Cisco IOS software image that contains the fix for caveat CSCeg07394. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07394. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: There is no workaround.

- CSCeh35457

  Symptoms: A policy map may be removed from an ATM PVC range configuration without a check for an exact match of the policy map name. This situation may cause the wrong policy map to be removed from the ATM PVC range configuration.

  Conditions: This symptom is observed when you enter the **no service-policy output** *policy-map-name* command on a subinterface that is administratively shut down. Any policy map that is attached to this subinterface may be deleted, regardless of whether or not the name of the policy map that is removed matches with the name of the policy map that should be removed. The symptom occurs only in a PVC range configuration on ATM subinterfaces.

  Workaround: There is no workaround.

- CSCeh35823

  Symptoms: When a router detects "invalid identity" failures while decrypting IPsec packets, a memory leak occurs for the packet memory that is associated with these failed packets.

  Conditions: This symptom is observed only when an "invalid identity" error occurs, which is an uncommon error that indicates that the originating router does not send packets according to what was originally negotiated. However, if there is another error that causes a "bad" decryption, the packet could be invalid and may also cause the symptom to occur.

  Workaround: There is no workaround.

- CSCeh36391

  Symptoms: The line protocol on a serial link stays down and input CRC errors are generated.

  Conditions: This symptom is observed when a T1 WIC is connected to a 56K DSU WIC via a switch and mux, when the switch provides the clock, and when the **network-clock-select** command is enabled on the T1 WIC side to route the clock to the TDM backplane.

  Workaround: There is no workaround.

- CSCeh37039

  Symptoms: A file system fails to complete the **dir** command or a **show** command upon encountering a unrecognized file.

  Conditions: This symptom is observed when there is a file of a type that is unrecognizable or not supported by the USB token file system.

  Workaround: Format the USB token prior to its first use.

- CSCeh37340

  Symptoms: Accounting does not start after a tunnel goes down and comes back up again.

  Conditions: This symptom is observed when multiple clients are connected to a head-end router through a platform that is configured for NAT.

  The tunnel interface should be down when clients try to re-key an IPSec SA and accounting should fail. After the permitted number of re-key attempts, the IKE SA and peer structures should be eliminated. However, when the tunnel interface goes up and IKE negotiation starts again, accounting should also start again.

  Workaround: There is no workaround.

- CSCeh39561

  Symptoms: A fax call may be stuck in the RINGING, ACTIVE, or FXSLS_WAIT_RELEASE_REQ state.

  Conditions: This symptom is observed on a Cisco router that is configured for VoIP and fax relay during a test that includes call waiting.

  Workaround: There is no workaround.

- CSCeh40183

  Symptoms: A router reloads unexpectedly when the **show policy interface** EXEC command is entered.

  Conditions: This symptom is observed on a Cisco router when two users are connected to the router and simultaneously enter the **show policy interface** EXEC command.

  Workaround: Ensure that only one user at a time enters the command.

- CSCeh41272

  Symptoms: After you perform an OIR of a PA-SRP-OC12 port adapter on a Cisco 7200 series, the router may not show any nodes in the SRP ring and may stop forwarding traffic. with IOS release

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13) or Release 12.3(11)T3.

  Workaround: There is no workaround.

- CSCeh41997

  Symptoms: EEM Tcl policies leak a significant amount of memory every time they run.

  Conditions: This symptom occurs because the memory model that is currently implemented in Cisco IOS software that supports Tcl assumes a single threaded model in which global memory is not released when the Tcl script completes.

  Workaround: There is no workaround.

- CSCeh42620

  Symptoms: Authentication, Authorization, and Accounting (AAA) for IKE fails with the following message when trying to begin session accounting:

  ```
  ISAKMP AAA: Unable to allocate AAA User ID: no peer
  ```

  Conditions: This error occurs when IKE accounting is configured in a site-to- site IPSec VPN. It will not occur when IKE accounting is configured in conjunction with mode configuration, XAUTH or EZVPN.

  Workaround: There is no workaround.

- CSCeh42852

  Symptoms: A T.37 fax fails on a Cisco 2800 series because of clocking problems with a BRI. The fax that is sent or received via the BRI may be incomplete with cut pages or a part lost. About 40 to 50 percent of the faxes fail.

  Conditions: This symptom is observed in the following topology:

  A fax is sent from a fax machine via the PSTN to a BRI on a Cisco 2800 series. The Cisco 2800 series connects via an IP interface to an SMTP mail server.

  Workaround: There is no workaround. Note that a fax that is sent via FXS instead of via a BRI goes through fine.

- CSCeh43531

  Symptoms: A Cisco Catalyst 6000 series or Cisco 7600 series that is configured with a VPN Services Module (VPN SM) may reload during the processing of many IPSec tunnels under stress.

  Conditions: This symptom is observed when the Cisco Catalyst 6000 series and Cisco 7600 series that are configured with a dynamic crypto map and Dead Peer Detection (DPD).

  Workaround: There is no workaround.

- CSCeh45653

  Symptoms: There are several symptoms:

  – The Embedded Event Manager (EEM) does not pass a configured session user name in a callback via an EEM applet.

  – An EEM applet does not correctly interact with the CLI library.

  When you enter the **action cli** applet configuration command, the router to crash because the TTY output buffers are not null-terminated.

  Conditions: These symptom are observed when you use TACACS authentication and when an EEM applet that interact with the CLI library through the **action cli** applet configuration command is triggered.

  Workaround: Disable TACACS authentication.

  Alternate Workaround: Configure an EEM script to perform the same EEM actions as the EEM applet.

- CSCeh45841

  Symptoms: A router crashes when you enter the **debug voip dialpeer detail** command while a voice port that belongs to a trunk group is shut down or brought up.

  Conditions: This symptom is observed on a Cisco router that functions as a voice gateway when the voice port belongs to a trunk group such as a PSTN trunk group and when the voice port is shut down by entering the **shutdown** command or brought up by entering the **no shutdown** command.

  Workaround: Do not enter the **debug voip dialpeer detail** command while a voice port that belongs to a trunk group is shut down or brought up.

- CSCeh46004

  Symptoms: A SAR ucode reload is not recorded.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF when you enter a command that causes a reload of the SAR microcode.

  Workaround: Check the log for references to the SAR ucode reload.

- CSCeh47169

  Symptoms: A router crashes when you enter the **service-module content-engine** *slots/unit* **reset** command followed by the **service-module content-engine** *slot/unit* **session** command.

  Conditions: This symptom is observed on a Cisco 2851, Cisco 3745, and Cisco 3845.

  Workaround: There is no workaround.

- CSCeh49205

  Symptoms: Ping fails after you enter the **ip cef accounting** command.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that is configured for MPLS VRF.

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

First Alternate Workaround: Reload the PXF engine by entering the **microcode reload pxf** command.

Second Alternate Workaround: Reload the RPM-XF.

- CSCeh49462

  Symptoms: Tracebacks are generated on a Cisco AS5850 that is configured for analog and digital bulk calls.

  Conditions: This symptom is observed on a Cisco AS5850 that is configured with ERSCs and that functions under stress.

  Workaround: There is no workaround. However, the symptom does not impact service because the calls are processed by the Cisco AS5850.

- CSCeh50570

  Symptoms: A Cisco platform reloads when you bring up bulk asynchronous and digital SS7/VPDN calls.

  Conditions: This symptom is observed on a Cisco AS5850.

  Workaround: There is no workaround.

- CSCeh51250

  Symptoms: A Cisco 2800 series may display tracebacks and generate a spurious memory access, and some of the terminal lines in the output of the **show line** command may be missing.

  Conditions: This symptom is observed on a Cisco 2800 series that is configured with an HWIC-16A WAN interface card and an NM-32A network module.

  Workaround: There is no workaround. Note that the symptom does not occur on a Cisco 3845 that functions in the same configuration.

- CSCeh51368

  Symptoms: When a CBR or VBR PVC that is configured on DSL interfaces is changed to an UBR PVC, traffic handling may become unpredictable, in particular when the tx-ring setting has a small value.

  Conditions: This symptom is observed on a Cisco 2800 series.

  Workaround: Only use a CBR or VBR PVC.

- CSCeh51606

  Symptoms: A router crashes when you enter the **clear ip nat nvi trans vrf services forced** command to clear the NVI instances of NAT translations.

  Conditions: This symptom is observed on a Cisco router that is configured for VRF services and NAT translation with a static source address.

  Workaround: There is no workaround.

- CSCeh54615

  Symptoms: LSPs that support AToM circuits may fail to come up.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that includes the fix for DDTS ID CSCeg74562. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74562. 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.

- CSCeh54816

  Symptoms: L2 policing does not function properly for certain packet sizes because the policing byte counter shows that a cRTP packet uses more cells than it does. For example, if a cRTP packet of 73 bytes uses two cells, the policing byte counter may show that the cRTP packet uses three cells.

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-XF when a policy map with a non-realtime class is attached to a multilink interface that is configured for cRTP.

  Workaround: There is no workaround.

- CSCeh55113

  Symptoms: A Cisco MGX 8800 series RPM may reload.

  Conditions: This symptom is observed when the RPM processes a heavy traffic load and when the CPU use is close to 100 percent.

  Workaround: Do not overload the RPM.

- CSCeh56312

  Symptoms: Packets are not shaped when traffic shaping is configured on a tunnel interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBA but may also occur in other releases.

  Workaround: Configure class-based shaping. If this is not an option, there is no workaround.

- CSCeh56358

  Symptoms: Missing entries in an MPLS forwarding table cause a ping failure.

  Conditions: This symptom is observed when the following events occur in an MPLS environment:

  – One router (router A) learns about a second router (router B) via a third router (router C) and router B has the **no mpls ip** global configuration command enabled. Between router A and router B, there is also an interface that is initially in the shutdown state and that has the **mpls ip** interface configuration command enabled.

  – The connection between router A and router C is dropped and the interface between router A and router B is brought up by entering the **no shutdown** interface configuration command.

  – The expected behavior is that router A learns about router B directly from router B and that router A updates its LFIB with “Untagged” as the outgoing label because router B has the **no mpls ip** global configuration command enabled. However, this does not occur: the LFIB of router A is not updated properly, causing incoming labeled packets on router A to be dropped.

  Workaround: Enter the **clear ip route** *network* EXEC command on router A.

- CSCeh56402

  Symptoms: A router may crash when you shut down the Frame Relay interface of a peer.

  Conditions: This symptom is observed on a Cisco router that connects to the peer via a serial interface that has Frame Relay encapsulation and encryption enabled.

  Workaround: There is no workaround.

- CSCeh60700

  Symptoms: A router that is configured for GRE+IPSec tunnel protection and VRF drops packets that are larger than the size of the MTU of the tunnel interface. The router should fragment the packets.

  Conditions: This symptom is observed on a Cisco 2600 series when the size of a (cleartext) packet is larger than 1434 bytes (which is the Ethernet MTU minus the IPSec overhead). However, the symptom is platform-independent and occurs with both software encryption and onboard hardware encryption engines.

Workaround: On the tunnel interface that is configured for GRE+IPsec tunnel protection and VRF, configure an MTU size that is smaller than the MTU size of the physical interface of the tunnel source minus the IPSec overhead, as in the following example:

```
interface tunnel0
ip mtu 1400
```

(This example assumes that the physical interface of the tunnel source is an Ethernet interface with an MTU of 1500 bytes.)

- CSCeh61337

  Symptoms: You can change the *milliseconds* argument of the **ip icmp rate-limit unreachable** *milliseconds* command or the **ip icmp rate-limit unreachable DF** *milliseconds* command, but the new time limit does not take effect even though the configuration reflects the new time limit.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs a Cisco IOS Release 12.3(11)T5 or an earlier 12.3T release.

  Workaround: There is no workaround.

- CSCeh61775

  Symptoms: You cannot easily detect any rewrite string errors in the multicast FIB.

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-XF that is configured for PXF forwarding. If multicast packets are dropped, you cannot detect a programming inconsistency in multicast FIB rewrite strings while debugging.

  Workaround: Compare the outputs of the **show pxf cpu mroute** and **show ip mroute** commands an check for any inconsistencies in the rewrite strings.

- CSCeh62596

  Symptoms: A Telnet session may pause indefinitely after 13 characters or carriage returns have been accepted.

  Conditions: This symptom is observed on a Telnet session through a PVC that is configured for PPP over ATM (PPPoA).

  Workaround: If possible, use a Fast Ethernet interface for the Telnet session.

- CSCeh62694

  Symptoms: Before you start a BACD script, you cannot log out all agents from an ephone hunt group and activate the Do Not Disturb (DND) feature.

  Conditions: This symptom is observed on a Cisco gateway that has an ephone hunt group configured.

  Workaround: There is no workaround.

- CSCeh65386

  Symptoms: If a crypto map has RRI enabled and is applied to more than one interface, removing the map from one interface removes all active routes that are associated with other instances of this crypto map. In particular, this situation affects dialup termination and VPN connectivity on the same physical router. When you use a virtual template, the disconnection of one virtual-access interface that is spawned from the virtual template causes all routes for all other virtual-access interfaces to be removed.

  Not all IKE and IPSec SAs on active connections are impacted, and when IPSec is rekeyed, routes are restored on the active interfaces.

  Conditions: These symptoms are observed on a Cisco router under he following conditions:

  – The same crypto map is applied to multiple interfaces.

  - RRI is configured on the crypto map.
  - VPN and dialup are configured on the same physical router.
  - There are active IPSec SAs and routes.

  Workaround: Do not remove a crypto map from an interface when there are active connections on other interfaces that use the same crypto map. First clear all SAs from the crypto map and then remove the interface.

- CSCeh66909

  Symptoms: A 6PE router crashes during an IPv6 ping to another PE router at the far side of a network.

  Conditions: This symptom is observed when you enter the **no mpls ipv6 source-interface** command followed by the **no interface** *type number* command and when the *type number* argument of the **no interface** *type number* command is the same IPv6 source interface that was used in the **mpls ipv6 source-interface** command.

  Workaround: When you disable the preferred IPv6 source interface, first delete the IPv6 interface by entering the **no interface** *type number* command and then enter the **no mpls ipv6 source-interface** command.

- CSCeh67427

  Symptoms: A router crashes when you configure a large number of E1 PRIs.

  Conditions: This symptom is observed rarely on a Cisco 3800 series and may be related to timing.

  Workaround: There is no workaround.

- CSCeh67651

  Symptoms: The policy map output counters are incorrect. The counters do not show the total number of packets, that is, the number of transmitted plus dropped packets is smaller than the number of incoming packets.

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-XF only when congestion occurs for non-LLQ classes, excluding the default class. On the RPM-XF, IPHC is configured on a multilink interface with a policy map that has four classes (one LLQ, two non-LLQ, and one default class), traffic enter for all classes, and each class has random or tail drops.

  Workaround: There is no workaround.

- CSCeh67918

  Symptoms: When you enter the **show fabric channel-counters** command on the supervisor engine or MSFC, the CMM may crash and generate the following error message:

  ```
  %SYS-3-BADBLOCK: Bad block pointer 646886B8
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series that runs Cisco IOS Release 12.3(8)XY4 or Release 12.4 and that has a Switch Fabric Module (SFM) or Supervisor720, which has a built-in switch fabric module.

  Workaround: Do not enter the **show fabric channel-counters** command. Note that this command is also part of the **show tech-support** command.

- CSCeh68537

  Symptoms: A Cisco 2600 series crashes when the user-locale is configured as JP.

  Conditions: This symptom is observed on a Cisco 2600 series that is configured with 256 MB of memory. The symptom is caused by creation of the large file that is required for the JP font, kate, and dictionary XML files.

Workaround: There is no workaround.

- CSCeh69534

  Symptoms: A router crashes when you enter the **show crypto pki timers** or **show crypto ca timers** command.

  Conditions: This symptom is observed on a Cisco router that has PKI configured for IKE authentication.

  Workaround: Do not enter the above-mentioned commands.

  First Alternate Workaround: Reissue all certificates to ensure that CDPs do not contain non-alphanumeric printable ASCII characters such as blanks.

  Second Alternate Workaround: Do not use PKI for IKE authentication.

- CSCeh72180

  Symptoms: A router may unexpectedly reload and generate the following error message:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x60FB1F70
  ```

  Conditions: This symptom is observed on a Cisco 7200 series when one interface is configured for IP Header Compression (IPHC) and when another interface has a crypto map that includes the **qos pre-classify** command. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeh73049

  Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at

  http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

- CSCeh76239

  Symptoms: Web Cache Communication Protocol (WCCP) may fail.

  Conditions: This symptom is observed on a router that is configured with IPSec, CBAC (that is, the **ip inspect** command is enabled), and NAT. One specific scenario in which WCCP fails is when a single interface is configured to terminate one or more IPSec tunnels and has the **ip nat outside source** command, **ip inspect out** command, and **ip wccp web-cache redirect out** command enabled.

  Workaround: When the **ip inspect out** command is enabled on the WCCP-redirected interface but the **ip inspect in** command is not configured on the client interface, configure a WCCP redirect list that excludes the address of the WCCP-redirected interface.

- CSCeh78358

  Symptoms: A Cisco MGX RPM-PR resets because of the expiration of a watchdog timer.

  Conditions: This symptom is observed when the Tx or Rx SAR of the RPM-PR crashes.

  Workaround: There is no workaround.

- CSCeh78411

  Symptoms: If a spoke cannot complete IKE phase I because of a bad certificate, the failed IKE sessions may not be deleted on an IPSec/IKE responder. Such failed sessions may accumulate, eventually causing router instability. These failed sessions can be seen in the output of the **show crypto isakmp sa | i MM** command:

```
172.18.95.21    10.253.34.80   MM_KEY_EXCH        898    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        896    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        895    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        894    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        893    0 ACTIVE
...
```

  Conditions: These symptoms are observed when RSA signatures are used as the authentication method.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that is used for the IKE sessions or re-apply the crypto map to this interface.

- 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.

- CSCeh87889

  Symptoms: A router that has one manually-configured L2TPv3 Xconnect session crashes when it receives an SCCRQ message from its remote peer.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(1.8) or Release 12.4(1.8)T and that functions as a PE router (PE2) in the following topology:

```
CE1 --- PE1 ---- PE2 --- CE2
```

  The symptom occurs when a signaled L2TPv3 Xconnect session is configured on PE1.

  Workaround: Ensure that the manually-configured L2TPv3 Xconnect session is not the first configured session.

- CSCeh90336

  Symptoms: When EzVPN client is configured in network extension mode with more than one inside ACL and when the server has split-tunneling configured, traffic that originates from a source address via an inside ACL is no longer NATted, preventing access to the Internet.

Conditions: This symptom is observed only when multiple inside ACLs are configured and does not occur when a single inside ACL is configured. The symptom is not platform specific.

Workaround: There is no workaround.

- CSCeh91772

  Symptoms: If an existing file is extended, an ATA file system may become corrupted. When this situation occurs, the output of the **dir** command or of a **show** command does not list the files because the files are corrupted.

  Conditions: This symptom is observed when you enter any command that extends a file such as the **show interfaces ethernet | append disk0:file** command.

  Workaround: Do not enter a command that extends a file.

- CSCeh92060

  Symptoms: When more than one voice calls is made, one-way voice occurs in the direction of a CE router to a PE router for one or more of the calls because the voice packets are not transmitted past the PE router. The output of the **show ip rtp header-compression** *interface-type interface-number* command shows many packet errors on the PE router.

  Conditions: This symptom is observed on a Cisco 8800 series MGX RPM-XF that functions as a PE router and that is configured with a multilink interface that has compression enabled.

  Workaround: There is no workaround.

- CSCeh94557

  Symptoms: When you reload a platform that generates calls and that is connected to a Cisco AS5400 or Cisco AS5850, some controllers fail to come up.

  Conditions: This symptom is observed when a platform that generates digital calls and a platform that generates analog calls are connected via a Cisco AS5400 or Cisco AS5850.

  Workaround: Reload the AS5400 or Cisco AS5850.

- CSCeh95884

  Symptoms: There is a three-second delay when a home agent (HA) replies to registration requests.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(14)T1 and that is configured for Mobile IP.

  Workaround: There is no workaround.

- CSCeh96861

  Symptoms: One-way audio or no audio may occur during a call that is made through a Cisco AS5400.

  Conditions: This symptom is observed when the Cisco AS5400 functions as a terminating gateway and is connected to a Cisco 3600 series or Cisco 3800 series that functions as an originating gateway. All platforms run Cisco IOS Release 12.3(14)T. The symptom may also occur in later releases.

  Workaround: Enter the **playout-delay nominal 200** command on the voice port that is used for the call.

- CSCeh97080

  Symptoms: When Multiprotocol Label Switching (MPLS) is enabled on a router, one or more LDP sessions may be disrupted during periods of extremely high CPU use.

  Conditions: This symptom is observed when the CPU use of the router temporarily increases to more than 90 percent for several tens of seconds and when one or more high-priority processes are frequently active but do not necessarily use many CPU cycles.

For example, high CPU use may occur when a peer router is reloaded or when an interface with several hundreds of numbered IP subinterfaces comes up, which causes many processing changes on the router because of the "Tagcon Addr" process.

On a Cisco 12000 series, high CPU use may occur because of the "Fabric ping" high-priority process, which is frequently active.

Other high-priority processes may also cause the symptom to occur.

Workaround: To increase the length of the hello adjacency holdtimes, enter the **mpls ldp discovery hello holdtime** command on the affected router. You may need to enter this command on all platforms in the network in order to provide full protection.

- CSCei01321

  Symptoms: You cannot bring up a serial interface of a channelized E1 or T1 port. The interface remains in the down/down state.

  Conditions: This symptom is observed on a Cisco 3600 series.

  Workaround: There is no workaround.

- CSCei02290

  Symptoms: The WRED threshold increases nine times from the configured value. If this situation occurs repeatedly, the WRED threshold configuration may eventually disappear.

  Conditions: This symptom is observed on a Cisco MGX 8800 series that is configured with two RPM-XFs when XFL is configured on the active RPM-XF and a switchover occurs on the standby RPM-XF.

  Workaround: There is no workaround.

- CSCei03508

  Symptoms: A software-forced reload on a corrupted redzone block occurs on a router.

  Conditions: This symptom is observed on a Cisco 2800 series when you configure IPSec.

  Workaround: Do not configure IPSec on the router.

- CSCei04017

  Symptoms: Multicast traffic may not pass through an L2TPv3 tunnel. Because multicast hello packets do not pass either, an OSPF or EIGRP neighbor may not come up.

  Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.4(1), that functions as a PE router, and that is configured for L2TPv3.

  Workaround: There is no workaround.

- CSCei05553

  Symptoms: A Modular QoS CLI (MQC) CoS marking disappears after you reload a router and QoS does not work.

  Conditions: This symptom is observed on a Cisco router when the policy map is configured with a class using CoS marking via the **set cos** command. After the router has reloaded, the CoS marking is still present in the configuration but does not appear in the output of the **show policy-map interface** command.

  Workaround: Remove and re-apply the service policy on the main interface.

- CSCei08347

  Symptoms: When you ping a Gigabit Ethernet (GE) interface on an NPE-G1 that has the **ip pim sparse-mode** or **ip pim sparse-dense-mode** command enabled, the ping fails.

Conditions: This symptom is observed on a Cisco 7200 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the GE interface of the NPE-G1.

Workaround: After you have shut down and brought up the GE interface, enter the **no ip pim sparse-mode** or **no ip pim sparse-dense-mode** command and then reconfigure the command.

- CSCei08458

  Symptoms: The FIB may be disabled or the output interface may be stuck on an A3 ATM port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dLFIoATM.

  Workaround: Reload the microcode or perform an OIR to recover the A3 ATM port adapter.

- CSCei22930

  Symptoms: On a router that is configured with an IMA interface, QoS configurations may be ignored and deleted from the IMA interface, and the router may generate the following error messages and tracebacks:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  -Traceback= 611D46E8 6002160C 61D4EF90 602C329C 602C6574 602C6D40 61D52170 61D54F2C
  61D553E8 61D55784 61D6FF84 61D550EC 61D5516C 604818FC 6047E89C 6047E9C8

  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
  -Traceback= 611D46E8 600177F4 6145DCB4 6145DDFC 6146B8E8 6146E174 616AB8B0 616ABB58
  6205C598 62066DE0 6205C640 61D557F0 61D6FF84 61D550EC 61D5516C 604818FC

  %SYS-2-MALLOCFAIL: Memory allocation of 19 bytes failed from 0x6145DCAC, alignment 0
  Pool: Processor  Free: 139749528  Cause: Interrupt level allocationAlternate Pool:
  None  Free: 0  Cause: No Alternate pool
  -Process= "<interrupt level>", ipl= 1, pid= 3
  -Traceback= 611D46E8 60012958 6001822C 6145DCB4 6145DDFC 6146B8E8 6146E174 616AB8B0
  616ABB58 6205C598 62066DE0 6205C640 61D557F0 61D6FF84 61D550EC 61D5516C
  ```

  Conditions: This symptom is observed on a Cisco router that has an NM-ATM T1 or E1 network module that is configured with an IMA interface and an IMA group when the IMA interface has both the **atm bandwidth dynamic** command and a QoS configuration enabled. The symptom occurs when link flaps and when the bandwidth is changed.

  Workaround: Do not enter the **atm bandwidth dynamic** command on an IMA interface that has a QoS configuration.

  Alternate Workaround: Configure the bandwidth of the IMA interface to be lower than the total bandwidth of all UNI interfaces of the IMA group.

- CSCei23461

  Symptoms: When you reboot a router that is configured with an NM-32A network module, a software-forced crash may occur.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T. When you remove the cabling from the NM-32A network module, the router boots without any problem.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(8)T6.

- CSCei33881

  Symptoms: The following error message is generated when you attempt to configure tunnel protection on an IPIP tunnel:

  ```
  ERROR: tunnel protection is only valid on IPIP, GRE, and MGRE interfaces
  ```

  This situation prevents tunnel protection from functioning on an IPIP tunnel.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T or Release 12.4.

Workaround: There is no workaround.

- CSCin67253

  Symptoms: A Cisco 7500 series may stop forwarding traffic via an Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) that is configured on an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+).

  Conditions: This symptom is observed on a Cisco 7500 series that has a PA-MC-8TE1+ that is configured for Frame Relay over Multiprotocol Label Switching (FRoMPLS) or Frame Relay/ATM/Ethernet interworking when you perform an online insertion and removal (OIR) of the Versatile Interface Processor (VIP) in which the PA-MC-8TE1+ is installed.

  Workaround: Remove and reconfigure the affected AToM VC.

- CSCin67741

  Symptoms: A Route Processor (RP) crashes when encapsulation is removed by entering the **no encapsulation** command.

  Conditions: This symptom is observed on a multilink interface that is configured for DLFI and that processes traffic.

  Workaround: There is no workaround.

- 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.

- CSCin77189

  Symptoms: When a voice call is made via the G726r16 or G726r24 codec via a Cisco Multiservice IP-to-IP Gateway (IPIPGW) using H.323-to-SIP interworking, the following symptoms may occur:

  – The originating party does not hear the ringback tone.
  – Both the originating and terminating party do not hear voice because the voice path was not established.

  Conditions: This symptom is observed when H.323 is configured to use a static payload type for the G726r16 or G726r24 codec and when SIP is configured to use a dynamic payload type for the G726r16 or G726r24 codec. This situation causes a mismatch of payload type for the G726r16 or G726r24 codec.

  Workaround: There is no workaround.

- CSCin82582

  Symptoms: After you have reloaded a Cisco 3745 that is configured with ATM AIM cards and that has a startup configuration that includes BERT functionality, a software-forced reload may occur on the router and the router does not come up.

  Conditions: The symptom is observed on a Cisco 3745 that runs Cisco IOS interim Release 12.3(12.12)T1 when the codecs that are included in the startup configuration are LLCC. The software-forced reload does not occur after you have reloaded the router with the default

configuration, that is, when codec information is not included and when ATM AIM cards are not configured. The router crashes only when all the voice ports are initialized and ATM AIM cards are in use.

Workaround: There is no workaround.

- CSCin84542

  Symptoms: A VWIC multiflex trunk controller may not come up.

  Conditions: This symptom is observed when you boot a Cisco 3745 that runs Cisco IOS Release 12.3(7)T6. This problem will only occur with **alarm trigger-blue** command enabled

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected controller after the router has booted.

- CSCin85528

  Symptoms: A router crashes during a conference call.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured with a DSP Farm.

  Workaround: There is no workaround.

- CSCin86322

  Symptoms: An end-to-end sweep ping fails across a dLFI bundle and the bundle flaps.

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

  Workaround: There is no workaround.

- CSCin86923

  Symptoms: A PVC is unexpectedly removed from an IMA interface when one or more IMA links go down.

  Conditions: This symptom is observed on a Cisco router when the bandwidth that is configured for the PVC cannot be supported after one or more IMA links go down.

  Workaround: Reconfigure the PVC with a bandwidth that can be supplied by the remaining IMA links.

- CSCin88077

  Symptoms: An active SP becomes stuck with an “slcp process” error when you enter the **test crash** command on the active RP.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series that is configured with an ATA file system but is not platform-specific. The symptom occurs because of an error in the ATA file system.

  Workaround: There is no workaround.

- CSCin88273

  Symptoms: After an RPR+ or SSO switchover occurs, an MLP sequence number mismatch may occur, a ping between back-to-back interfaces may not go through, and the routing protocol through this link may go down.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMLP and RPR+ or SSO.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the multilink interface of the Cisco 7500 series.

- CSCin88303

  Symptoms: The line protocol of unchannelized interfaces on a PA-MC-2T3+ port adaptor remains down although the link is up.

  Conditions: This is observed when you change from the channelized mode to the unchannelized mode by entering the **no channelized** command on the T3 controller of the PA-MC-2T3+ port adaptor.

  Workaround: There is no workaround.

- CSCin88417

  Symptoms: Transmit accumulator loss may occur for MLP interfaces after you have performed an OIR of a VIP. When the transmit accumulator value goes to zero, MLP may stop forwarding or packets may be switched by dCEF.

  Conditions: This symptom is observed after you have performed an OIR of a VIP while traffic is running on MLP bundles.

  Workaround: Reload the VIP again and ensure that no traffic leaves from the MLP bundles immediately after the VIP comes up.

- CSCin88665

  Symptoms: A back-to-back ping fails on a Cisco 7500 series that has Multilink PPP (MLP) configured on serial interfaces of a PA-MC-STM-1 port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 only when MLP is configured on the serial interfaces.

  Workaround: Unconfigure MLP on the serial interfaces.

- CSCin89043

  Symptoms: A VIP may pause indefinitely or quality of service (QoS) may not work as expected on an interface that is configured for distributed MLP (dMLP).

  Conditions: This symptom is observed on a Cisco 7500 series when the VIP processes dMLP and LFI traffic.

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

- CSCin89146

  Symptoms: The G.728 codec calls fail on a SIP call leg of an IPIPGW.

  Conditions: This symptom is observed when the G.728 codec is configured on the SIP leg and when a “ptime” translation error occurs.

  Workaround: There is no workaround.

- CSCin89165

  Symptoms: SSG does not create host objects in RADIUS proxy mode.

  Conditions: This symptom is observed when SSG is configured in SSG proxy mode with the session identifier as IP.

  Workaround: Use other parameters apart from IP as the session identifier. If this is not a practical option, there is no workaround.

- CSCin89549

  Symptoms: A router that is configured for IPSec may crash while processing an AAA authorization reply.

Conditions: This symptom is observed on a Cisco router that is configured to skip AAA Authentication (Xauth) when the AAA authorization reply contains per-user attributes such as an IPV4 address.

Workaround: Change the AAA user database to not return per-user attributes when Xauth is not configured.

- CSCin90300

  Symptoms: Controllers do not come up after you have manually configured the card type for a PA-VXC-2TE1+ port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS interim Release 12.4(0.6) but may also occur in Release 12.3.

  Workaround: Reload the router to enable the controllers come up.

- CSCin91163

  Symptoms: Packets may be dropped as reassembly drops on a distributed (dMLP) ingress interface that has interleaving configured.

  Conditions: This symptom is observed on a PA-MC-STM-1 port adapter when more than two DS0 members are part of an dMLP bundle that is configured for interleaving.

  Workaround: There is no workaround.

- CSCin91267

  Symptoms: You may not be able to bind interfaces to an uplink or downlink.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG.

  Workaround: There is no workaround.

- CSCin91843

  Symptoms: Auto-logon services do not automatically log on when you connect via a Service Selection Gateway (SSG).

  Conditions: This symptom is observed when the user profile that is downloaded via the Access-Accept response from a RADIUS server contains a netmask (RADIUS attribute 9) that is smaller than 32 bits and when the SSG functions in PBHK mode.

  Workaround: Increase the netmask bits in such a way that the bitwise and ampersand (&) operation between the netmask and the SSG PBHK source IP address results in an SSG PBHK source IP address without any alteration.

- CSCin91968

  Symptoms: An EzVPN client connection is reset, the connection goes down, and the following error message is generated:

  ```
  %CRYPTO-4-EZVPN_SA_LIMIT: EZVPN(ez) Ezvpn active SA count: 0 has crossed maximum limit of 0" is displayed.
  ```

  Conditions: This symptom is observed when an EzVPN profile does not contain the inside subnet configuration, that is, the ACL number or ACL name is not configured.

  Workaround: Create a dummy ACL entry that does not have an access list associated with it.

- 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.

- CSCsa44556

  Symptoms: When you remove and re-enter the **zone circuit-id** command, the command may not take effect.

  Conditions: This symptom is observed on a Cisco platform that functions as a gatekeeper.

  Workaround: Reload the gatekeeper after you have made the configuration changes.

- CSCsa44852

  Symptoms: A virtual-access interface flaps continuously.

  Conditions: This symptom is observed Cisco 3745 router that functions in a PPPoA environment during normal working conditions.

  Workaround: Disable keepalives on the dialer interface on the remote router.

- CSCsa47020

  Symptoms: When Multilink Frame Relay (FRF.16) is configured on two bundled serial links and when the traffic rate is above 2 Mbps, packet loss occurs.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7500 series when you send a 64-byte Ethernet frame. The symptom does not occur when the frame size is 512 bytes or more.

  Workaround: There is no workaround.

- CSCsa48259

  Symptoms: A router or switch may crash when you enter the **show crypto socket** command.

  Conditions: This symptom is observed on a Cisco router or switch that runs Cisco IOS Release 12.2(18) or Release 12.4 when a large number of tunnel interfaces are in the process of being shut down.

  Workaround: Wait until all of the tunnel interfaces are shut down before you enter the **show crypto socket** command.

- CSCsa53006

  Symptoms: A 3-port Gigabit Ethernet port adapter (EPA-GE/FE-BBRD) may crash with a redzone memory corruption that is related to the “tagsw_start_stats_process”, and messages similar to the following may be generated:

  ```
  %SYS-3-OVERRUN: Block overrun at 463BD398 (red zone 000010DF)
  %SYS-6-BLKINFO: Corrupted redzone blk 463BD398, words 10204, alloc 40ECCDA4, InUse,
  dealloc 0, rfcnt 2
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or a later release and that is configured for MPLS forwarding.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat is integrated in Cisco IOS software releases that do not support the Cisco 12000 series because the fix relates to the Tag Forwarding Information Base (TFIB) that is also used in other platforms.

- CSCsa53117

  Symptoms: Multi-Layer Switching (MLS) CEF may stop functioning when an interface status changes. Ping and connectivity problems may also occur.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series when you shut down an interface or change VRF routes and as a result no other interfaces can be provisioned.

  Temporary Workaround: Reload the supervisor engine.

- CSCsa56252

  Symptoms: When a cluster of Cisco CallManagers is used to control an SCCP gateway and a failover of the call manager occurs, the switchback to the primary Cisco CallManager may not occur properly for STCAPP endpoints. This situation may affect other SCCP endpoints besides STCAPP as well but this DDTS relates to endpoints that are controlled by STCAPP.

  Conditions: This symptom is observed when three Cisco CallManagers are configured. When two of the Cisco CallManagers are inactive, the third Cisco CallManagers is brought into service. When the primary Cisco CallManager is then brought into service, STCAPP endpoints do not register with the primary Cisco CallManager. Other permutations of the symptom may be possible with different numbers of Cisco CallManager in the cluster.

  Workaround: Do not home STCAPP endpoints to more than two Cisco CallManagers.

- CSCsa56901

  Symptoms: Cisco Fax Relay calls both to and from computer-based fax devices fail. Calls to and from traditional fax machines work fine. Calls to and from computer-based fax devices via the PSTN instead of via a Cisco Fax Relay network work fine too.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured for Cisco Fax Relay and VoIP.

  Workaround: There is no workaround.

- CSCsa57147

  Symptoms: A disconnect event is not thrown or caught on a Cisco AS5400.

  Conditions: This symptom is observed when the platform functions under a heavy load with a large number of calls that are disconnected from the gateway during VXML page execution. The disconnect event may not be thrown or get caught by the catch blocks of the root document.

  Workaround: There is no workaround.

- CSCsa59000

  Symptoms: A Cisco AS5850 reloads with an “unknown reload cause.”

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(10) when you enter the following commands:

  ```
  interface controller e1 1/17
  no extsig mgcp
  ```

  Workaround: There is no workaround.

- CSCsa59549

  Symptoms: A router that is configured for Content Based Access Control (CBAC) and Intrusion Prevention Systems (IPS) may unexpectedly reload.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T or a later release with a Cisco IOS firewall during session inspection under certain timing conditions.

Workaround: There is no workaround.

- CSCsa59667

  Symptoms: An AIM that is installed in a Cisco 2851 or Cisco 3845 may time out when it receives non-multiples of a 64-bits public key from a third-party vendor router. This situation causes the router to crash rather than verifying the key.

  The Cisco 2851 crashes because of a memory corruption. The Cisco 3845 crashes because of an "ALIGN-1-FATAL" bus error.

  Conditions: This symptom is observed on a Cisco 2851 and Cisco 3845 that run Cisco IOS Release 12.3(11)T3.

  Workaround: Ensure that the AIM receives multiples of the 64-bits public key.

  Alternate Workaround: Disable the AIM hardware encryption by entering the **no crypto engine aim 0** command. Doing so causes onboard encryption to occur.

- CSCsa60026

  Symptoms: Cells loss occurs on a single ATM link of PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

  Condition: This symptom is observed on a Cisco 7500 and 7200 series when one of the T1 or E1 member interfaces of an IMA group that is configured on a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter is disconnected or when you enter the **shutdown** command on one of these T1 or E1 member interfaces. The symptom is not platform-specific and may also occur in other releases.

  Workaround: There is no workaround.

- CSCsa61523

  Symptoms: The following error message is generated on a Cisco 7200 series that has Multilink PPP (MLP) configured on serial interfaces of a PA-MC-STM-1 port adapter:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(11)T3 only when MLP is configured on the serial interfaces. The symptom may also occur in Release 12.3 or 12.4.

  Workaround: Unconfigure MLP on the serial interfaces.

- CSCsa61635

  Symptoms: A Cisco router may reload unexpectedly because of a bad block pointer.

  Conditions: This symptom is observed on a Cisco 3660 that has a GRE tunnel configuration. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsa62681

  Symptoms: SIP messages from Cisco IOS gateways fail to reach the remote endpoint. This is seen for UDP transport only.

  Conditions: This symptom happens when interworking with a third party SIP device, which sends responses to SIP Requests to the source port of the request packet instead of sending them to the header port (5060). This is in violation of the RFC3261 rules for UDP (unreliable transports).

  Workaround: There is no workaround.

- CSCsa63019

  Symptoms: A security gateway may crash when ISAKMP accounting is enabled at aggressive time intervals such as 1-minute updates.

Conditions: This symptom is observed when ISAKMP accounting is enabled at very frequent update intervals together with ISAKMP NAT-T.

Workaround: Use ISAKMP accounting timers with a longer duration.

- CSCsa64885

  Symptoms: A router that is configured for SSG intermittently resets itself and generates a spurious memory access.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T with a prepaid or proxy service that has an idle or session timeout configured in the service profile.

  Workaround: There is no workaround.

- CSCsa65035

  Symptoms: The committed information rate (CIR) of policers is calculated incorrectly.

  Conditions: This symptom is observed when Frame Relay Traffic Shaping (FRTS) is applied using Modular QoS CLI (MQC) (that is, it is applied on the shaper in the parent service policy) and when the classes of the child policy include percentage-based policers.

  Workaround: There is no workaround.

- CSCsa65360

  Symptoms: During a high bit error rate (BER) condition, the controller of a PA-MC-8TE1+ port adapter remains up, which is not in compliance with the E1 and T1 standard.

  Conditions: This symptom is observed when BER data is injected into an E1 or T1 port of a PA-MC-8T1E1+ port adapter. The state of the controller does not change to DOWN after 10 seconds of a continuous severely errored seconds (SES) condition.

  Workaround: There is no workaround.

- CSCsa65656

  Symptoms: SSG uses a duplicate Acct-session-id (attribute 44) in a RADIUS accounting packet.

  Conditions: This symptom is observed for post-paid users.

  Workaround: There is no workaround.

- CSCsa66255

  Symptoms: IP data traffic does not pass via MLP.

  Conditions: This symptom is observed on a Cisco 3825 that runs the c3825-advsecurityk9-mz image of Cisco IOS Release 12.3(11)T3 when STAC compression on an AIM-COMPR4 fails.

  Workaround: There is no workaround.

- CSCsa66702

  Symptoms: A Cisco 3660 may reload when an IP phone is placed on hold.

  Conditions: This symptom is observed on a Cisco 3660 that runs Cisco IOS Release 12.3(11)T4.

  Workaround: There is no workaround.

- CSCsa67836

  Symptoms: A VIP or FlexWAN may crash with a TLB store exception on a Cisco 7500 series or a Cisco 7600 series.

  Conditions: This symptom is observed when the router is configured for distributed MFR and when the MFR bundle flaps while traffic is being processed.

  Workaround: There is no workaround.

Further Problem Description: This caveat is a timing issue: not all flaps cause the VIP or FlexWAN to crash.

- CSCsa68001

  Symptoms: All incoming packets on a Frame Relay Link have the DE bit set.

  Conditions: This symptom is observed on a Cisco 2811 that runs Cisco IOS Release 12.3 or Release 12.3(11)T2 under normal traffic conditions.

  Workaround: There is no workaround. Note that the symptom does not occur on a Cisco 1760 that runs Release 12.3(10).

- CSCsa68004

  Symptoms: A Service Selection Gateway (SSG) does not update tariff switch information to a user that logs in exactly at tariff switching time.

  Conditions: This symptom is observed for postpaid users only.

  Workaround: There is no workaround.

- CSCsa68228

  Symptoms: A Cisco router may crash when you enter the **dialplan-pattern** command.

  Conditions: This symptom is observed on a Cisco router that is configured with a high number of ephone-dns when you enter the **dialplan-pattern** command.

  Workaround: There is no workaround.

- CSCsa68768

  Symptoms: After a fallback occurs from a Cisco CallManager to a secure Survivable Remote Site Telephony (SRST) gateway, when a full-consult transfer occurs from a secure to a nonsecure IP phone and then back to a secure IP phone, all of which function in single-line mode, one-way voice is heard on one side and a loud noise is heard on the other side.

  Conditions: This symptom is observed only with a full-consult transfer system when there is a call transfer from a nonsecure IP phone to a secure IP phone.

  Workaround: Configure the IP phones to function in dual-line mode.

- CSCsa68978

  Symptoms: Memory allocation (malloc) failures may occur on a Cisco router that functions as a gatekeeper and that runs an H.323 stack.

  Conditions: This symptom is observed on the gatekeeper when gateways attempt to register a list of terminal aliases that consists of user names and H.323 IDs with the gatekeeper. The gatekeeper attempts to authenticate each terminal alias by allocating memory and sending an authentication request to the AAA server for each entry. Because the gatekeeper does not free the allocated memory when it receives a response from the AAA server, a memory allocation failure occurs eventually.

  Workaround: There is no workaround.

- CSCsa69464

  Symptoms: The **cns inventory** command does not function.

  Conditions: This symptom is observed on a Cisco 1700 series that runs a reformation image.

  Workaround: There is no workaround. Note that the command does function in regular Cisco IOS software images for the Cisco 1700 series.

- CSCsa69690

  Symptoms: The night service toggle code does not work properly with shared Directory Numbers (DNs).

  Conditions: This symptom is observed when the DN is shared on multiple phones.

  Workaround: There is no workaround.

- CSCsa71055

  Symptoms: Pings from a PE router to the Ethernet interface of a CE router fail.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that functions as a PE router and that runs Cisco IOS Release 12.3(2)XZ. The symptom could also occur in Release 12.3T.

  Workaround: Clear the IP route.

- CSCsa71310

  Symptoms: An E1 controller on an MGCP trunking gateway reports Loss of Frames (LOF).

  Conditions: This symptom is observed when you configure a Cisco 3660 as an MGCP trunking gateway.

  Workaround: There is no workaround.

- CSCsa71596

  Symptoms: The prompt file that is stored on an HTTP file server and that is invoked by a VXML document is not heard by a caller.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release 12.3(12.12)T5 when a VXML document attempts to retrieve and render a wav file that is stored on an HTTP file server.

  Workaround: There is no workaround.

- CSCsa71612

  Symptoms: When you make 21 calls and place one call on hold, the callee at the PSTN side does not hear the MoH.

  Conditions: This symptom is observed on a Cisco 2621XM and Cisco 3745 that run and IP voice image of Cisco IOS Release 12.3(7)T4 and that are configured with an NM-HD-2VE, a VWIC-1MFT-T1 or VWIC-2MFT-T1, codec complexity flex, and multicast MoH.

  Workaround: Add another NM-HD-2VE and configure codec complexity medium.

- CSCsa71793

  Symptoms: A Cisco 7200 series may reload because of a bus error when you enter a **show atm** command that accesses deleted VCs structures.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(12a).

  Workaround: There is no workaround.

- CSCsa71953

  Symptoms: Fast-start calls from an originating gateway (OGW) to a terminating gateway (TGW) via a Cisco Multiservice IP-to-IP Gateways (IPIPGW) fail when the tunnel is disabled at the TGW and extended caps are configured.

  Conditions: This symptom is observed on a Cisco 3700 series that functions as an IPIPGW.

  Workaround: Either disable or enable the tunnel on both the OGW and the TGW.

Alternate Workaround: Originate slow-start calls.

- CSCsa72085

  Symptoms: Two Cisco 7970 IP phones that function in secure SRST single line mode lose their secure mode.

  Conditions: This symptom is observed when the following sequence of events occurs:

  1. IP phone A calls IP phone B.
  2. IP phone B answers, causing IP phone A and IP phone B to be connected and secure.
  3. The Confirm button is pressed, causing "No line available" to be displayed because the mode is single line, not dual line. At this point, IP phone A and IP phone B are still connected and secure.
  4. Hold and resume is selected, causing the IP phones to lose their secure mode. The call is no longer secure.

  Workaround: There is no workaround.

- CSCsa72313

  Symptoms: The following error messages may be generated on a router that has IP ACL enabled:

  ```
  %SYS-2-INSCHED: suspend within scheduler
  -Process= "<interrupt level>", ipl= 3
  -Traceback= 40525388 40628848 4060AED4 403F15BC 403F34F8 403F37EC 400901C8 4008E730
  406A0EEC 40621120
  ```

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7200 series, Cisco 7304, and Cisco 7500 series when a Turbo ACL compilation is configured along with an ACL on an ingress interface and when traffic passes through the ingress interface. The symptom does not affect the Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsa72406

  Symptoms: One-way audio occurs when a conference/transcoding port adapter (WS-SVC-CMM-ACT) is used. However, a ping to the Fast Ethernet interface of the port adapter goes through.

  Conditions: This symptom is observed on a Cisco router or switch when the end points have a MAC address for which the signed addition of individual bytes is zero. The symptom occurs because the MAC address verification method of the WS-SVC-CMM-ACT is incorrect.

  Workaround: There is no workaround.

- CSCsa72425

  Symptoms: When Music on Hold (MOH) is not configured on a Cisco CallManager, placing an STCAPP-controlled voice port on hold causes the call to fail.

  Conditions: This symptom is observed when a caller uses the STCAPP-controlled voice port to call someone on the network who uses a Cisco 7960 IP phone and who places the call on hold before the inter-digit timeout arrives on the STCAPP-controlled voice port after the call is set up. (This timeout depends on the voice port settings.) Note that the symptom does not occur when the call is placed on hold after the inter-digit timeout arrives on the STCAPP-controlled voice port.

  Enter the **stcapp show device summary** command to view the state of the voice port. When the call is placed on hold, the state should transition to "ONHOOK_PENDING." When the inter-digit timeout arrives, the state changes to "OFFHOOK_TIMEOUT," indicating that the call is about to fail.

  Workaround: Configure MoH for the STCAPP-controlled voice port via the Cisco CallManager.

Further Problem Description: Another related problem is that when the call is placed on hold and the voice port is in the "ONHOOK_PENDING" state, pressing any digit on the phone starts the inter-digit timer automatically. When the inter-digit timeout occurs, the call transitions into the "OFFHOOK_TIMEOUT" state. The call fails shortly thereafter.

- CSCsa72784

  Symptoms: An incorrect frequency response may occur and may cause a distorted voice path on a voice port.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  – The affected port is on one of the following cards: VIC-4FXS/DID, VIC2-2FXS, VIC-2DID, VIC2-2E/M, NM-HDA-4FXS, or EM-HDA-8FXS.

  – Not all ports on the same card have the same impedance setting (for example, port 1/0 uses "600r" while port 1/1 uses "complex1").

  Workaround: Configure all ports for the same impedance value.

- CSCsa72951

  Symptoms: A DSMP-3-DSP_TIMEOUT error message may be generated when you place a fax call via a VoIP gateway.

  Conditions: This symptom is observed when the fax call is torn down and the gateway attempts to obtain call statistic information from the DSP. The DSMP state in this case is S_DSMP_COLLECTING_STATS as displayed in the error message. The timeout occurs only when MGCP PRI-backhaul mode is enabled. The symptom does not occur in standalone mode.

  The timeout itself does not impact the call for which it occurs because the timeout occurs at the end of the call while the call is being torn down and cleaned up. However, on some network modules, specifically, the 549 and 5421 DSP-based modules such as the NM-HDV and AIM network modules, when the timeout occurs, a DSP recovery mechanism is triggered and may impact other active calls on other channels on the same DSP as the one that reports the timeout. For this problem, caveat CSCsb14481 has been opened.

  Although the timeout may occur on a 5510-based DSP network module such as the NM-HDV2 network module, the DSP itself does not appear to be reset so no impact to other active calls is observed.

  To verify which DSP is currently in use on a gateway, enter the **show voice dsp** EXEC command.

  Workaround: When MGCP PRI-backhaul is configured in a Cisco CallManager environment, you can disable Fax Relay on a gateway to prevent timeouts from occurring by entering the **no ccm-manager fax protocol cisco** global configuration command on the gateway.

  Alternate Workaround: To prevent timeouts from occurring, configure the gateway to function in standalone mode.

- CSCsa73120

  Symptoms: A Cisco IPSec router may restart because of a bus error.

  Conditions: This symptom is observed when you remove a crypto map entry that includes the **dynamic** keyword in its definition, as in the following example:

```
router#show running
...
 crypto map map-name 5 ipsec-isakmp dynamic dyn-map
...
 router(config)#no crypto map map-name 5
```

Workaround: Before you delete the crypto map entry that includes the **dynamic** keyword in its definition, manually configure all dynamic crypto maps to point to a nonexistent ACL, as in the following example:

```
router#show running
...
 crypto dynamic-map dyn-map 5
...
 router(config)#crypto dynamic-map dyn-map 5
 router(config-crypto-map)#match address no-such-acl
```

- CSCsa73438

  Symptoms: When SSG functions in RADIUS proxy mode, SSG sends the RADIUS Framed IP Netmask Attribute value that it receives from a RADIUS server as the Framed IP Address Attribute value towards a GGSN or CSG downlink RADIUS client.

  Conditions: This symptom is observed when the RADIUS Framed IP Netmask Attribute value is less then a 32-bit mask.

  Workaround: Avoid using the RADIUS Framed IP Netmask Attribute or use a 32-bit mask value for it.

- CSCsa73587

  Symptoms: The **call application voice** *application-name* **uid-len** *number* does not function.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(0.6) and that is configured for IVR.

  Workaround: Enter the following sequence of commands:

  ```
  application
  service application-name
  paramspace uid-len number
  ```

- CSCsa73842

  Symptoms: An IP phone line is not released for some calls between Cisco CallManagers.

  Conditions: This symptom is observed when calls between the Cisco CallManagers are made via a Cisco Multiservice IP-to-IP Gateway (IPIPGW) that is configured for H.323.

  Workaround: There is no workaround.

- CSCsa74893

  Symptoms: An SSH server crashes when an SSH client attempts to connect to it.

  Conditions: This symptom is observed when the SSH server is configured to connect to a TACACS+ server for AAA authentication and when there is no TACACS+ server.

  Workaround: Configure a valid AAA authentication service on the SSH server.

- CSCsa78779

  Symptoms: A memory leak may occur in the processor memory pool of a router that runs encrypted traffic with an SA-VAM2.

  Conditions: This symptom is observed when the SA-VAM2 encrypts traffic and when underlying "no buffer" conditions exist in the I/O particle pools for the encrypted packets.

  Workaround: There is no workaround.

- CSCsa79551

  Symptoms: A Cisco AS5350 may leak memory while processing calls in an H.450 call-transfer scenario.

  Conditions: This symptom is observed on a Cisco AS5350 that runs Cisco IOS interim Release 12.4(0.6).

  Workaround: There is no workaround.

- CSCsa79580

  Symptoms: A Cisco AS5300 that is configured with a call switching module (CSM) may generate tracebacks that are related to a B-channel IDB. This situation may cause 64-kbps digital calls to be answered by modems instead of via High-Level Data Link Control (HDLC).

  Conditions: This symptom is observed on a Cisco AS5300 that runs Cisco IOS Release 12.3.

  Workaround: There is no workaround.

- CSCsa82222

  Symptoms: A Cisco router may reload because of a watchdog timeout in the SNMP engine process.

  Conditions: This symptom is observed on a Cisco 3700 series that runs Cisco IOS Release 12.3(6a) when you query the ifStackStatus MIB object. The symptom occurs because the query enters an infinite loop. Note that the symptom may be platform-independent.

  Workaround: Disable SNMP on the router.

- CSCsa82886

  Symptoms: A router crashes when you enter the **tftp-server** command.

  Conditions: This symptom is observed when the *filename* argument of the **tftp-server** command has a length of more than 67 characters.

  Workaround: Ensure that the length of the *filename* argument does not exceed 67 characters.

- CSCsa83881

  Symptoms: An interface of a PA-T3+ port adapter remains up during an Unavailable Seconds (UAS) condition that occurs because of a high C-bit or P-bit error rate.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-T3+ port adapter.

  Workaround: There is no workaround.

- CSCsa84724

  Symptoms: A buffer leak in the middle buffer pool may occur on a Communication Media Module (CMM).

  Conditions: This symptom is observed when the CMM is configured for Music on Hold (MoH).

  Workaround: Do not configure the CMM for MoH.

- CSCsa84972

  Symptoms: A voice gateway may crash because of a bus error. After the crash, the output of the **show version** command shows a message that is similar to the following:

  ```
  System returned to ROM by bus error at PC 0x612DDFC8, address 0x68000000
  ```

  (Note that the PC value can be different that the one shown above.)

  Conditions: This symptom is observed on a Cisco IAD2430 and Cisco VG224 that run Cisco IOS Release 12.3(14)T and that function as voice gateways.

Workaround: There is no workaround.

- CSCsa85839

  Symptoms: A Cisco Aironet AIR-AP1131AG-E-K9-P access point may not function because it does not receive power.

  Conditions: This symptom is observed when an EtherSwitch NM-16ESW-PWR network module or EtherSwitch NMD-36ESW-PWR network module does not detect and supply power to the AIR-AP1131AG-E-K9-P access point.

  Workaround: Use a power injector or external power supply.

- CSCsa86250

  Symptoms: The CPU utilization of a Cisco MGX series RPM-XF increases to 99 percent when a Gigabit Ethernet (GE) interface of a peer RPM-XF is shut down.

  Conditions: This symptom is observed when two RPM-XFs are connected via a GE interface. The affected side of the connection is configured with a 2-port GE card and peer is configured with a 1-port GE card.

  Workaround: There is no workaround.

- CSCsa86291

  Symptoms: Packets that enter on an interface that has the **ssg direction downlink** command enabled are not translated even though the **ip nat inside** is enabled.

  Conditions: This symptom is observed on a Cisco router that is configured for SSG with the TP, TT, or TX type of service and that runs Cisco IOS Release 12.3(11)T4 or Release 12.3(14)T. The symptom may also occur in Release 12.3 but does not occur in Release 12.3(11)T3.

  Note that when you disable the **ssg direction downlink** command on the interface, NAT works fine.

  Workaround: There is no workaround.

- CSCsa86918

  Symptoms: A clicking sound is heard after each .wav audio file is played from a VoiceXML (VXML) document.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.3(14)T only when there are multiple .wav files in a single VXML document and when the .wav files are concatenated together to play to the caller. The symptom does not occur for a VXML document that contains a single .wav file.

  Workaround: There is no workaround.

- CSCsa87076

  Symptoms: When an access control list (ACL) is applied to an EzVPN client configuration without being defined, a spurious memory access is generated and an IPsec SA does not come up.

  Conditions: This symptom is observed on a Cisco 1700 series that functions as an EzVPN client and that functions in “connect auto” mode.

  Workaround: Define the ACL before it is applied to the EzVPN client configuration and configure the “esp-3des esp-sha-hmac” transform set on the server to bring up the IPsec SA.

- CSCsa87811

  Symptoms: A memory leak occurs on an originating gateway.

  Conditions: This symptom is observed when Fast Start is enabled, when a call fails after the call proceeding has been received from a primary or alternate endpoint, and when the call falls back to the next alternate endpoint.

Workaround: There is no workaround.

Further Problem Description: The fast-start elements that are received in the call proceeding are freed only once for each call instead of being freed for each endpoint that is tried (assuming that the call falls back to alternate endpoints). This situation causes the memory leak.

- CSCsa88145

  Symptoms: In some scalability cases with a large number of tunnels, SVIs, or VLANs, FIB tracebacks occur after an SSO switchover.

  Conditions: This symptom is observed because traceback recording for the general event log and the interface event log is on by default.

  Workaround: There is no workaround. Note, however, that there is no functional impact.

  Further Problem Description: The fix for this caveat turns off traceback recording for the general event log and the interface event log.

- CSCsa89621

  Symptoms: The firewall performance of an NPE-G1 is below expectations, causing high CPU use.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(14)T1 and that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCsa91342

  Symptoms: A router may unexpectedly reload after the encapsulation is changed.

  Conditions: This symptom is observed when Internet Protocol Header Compression (IPHC) is configured on an interface and when you change the encapsulation.

  Workaround: There is no workaround.

- CSCsa91965

  Symptoms: A Cisco 7200 series that is configured for VoIP may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(1.1).

  Workaround: There is no workaround.

- CSCsa93883

  Symptoms: No error condition is detected when a properly structured IPv4 packet has an invalid version value in the IP header. For example, IPv4 packets that have a version value other than 4 are forwarded without an error.

  Condition: This symptom is platform-independent and occurs under normal operating conditions.

  Workaround: There is no workaround.

- CSCsa94064

  Symptoms: When the **speed** *kbps* argument of the **channel-group** *channel-group-number* **timeslots** *range* **speed** *kbps* controller configuration command is set to 64 kbps for a T1 channel group, the speed does not take affect and the T1 controller functions with the default speed of 56 kbps even though the output of the **show running-config** command shows that the controller is configured to function with 64 kbps.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release 12.3(11.7) or a later release, including Release 12.4, and that is configured with a T1 module.

Workaround: Select a channel-group number that is one number less than the timeslot range. For example, for a timeslot range of 10-22, select a channel-group number between 9-21 to enable the speed setting to function properly.

- CSCsa94162

  Symptoms: A DHCP client router has an old static route and a new static route concurrently. The output of the **debug dhcp detail** on the DHCP client router shows that the old static route is removed but that the routing table still contains the old static route. Also, the old static route is not removed after the static configuration is deleted.

  Conditions: This symptom is observed when a DHCP server renews the DHCP address and the DHCP gateway.

  Workaround: There is no workaround.

- CSCsa96494

  Symptoms: A call from an originating gateway (OGW) that is configured for SIP via an IPIPGW to a terminating gateway (TGW) that is configured for H.323 may fail when certain codecs are configured on the IPIPGW and H.323 TGW.

  Conditions: This symptom is observed under either one of the following conditions:

  – The SIP OGW is configured for g.711u, the IPIPGW for g.711u for both connections, and the H.323 TGW for g.729r8. In this configuration, the SIP OGW continues to use g.711u as the negotiated codec and discards the g.729r8 codec that is sent by the H.323 TGW via OLC.

  – The SIP OGW is configured for g.729r8, the IPIPGW for g.729r8 for both connections, and the H.323 TGW for g.711u. In this configuration, the SIP OGW continues to use g.729r8 as the negotiated codec and discards the g.711u codec that is sent by the H.323 TGW via OLC.

  Workaround: There is no workaround.

- CSCsa98462

  Symptoms: A Cisco router may display the following error messages and then reload because of a bus error:

  ```
  HDLC32_RX_ISR_ERR: no particles available! HDLC32_RX_ISR_ERR: no particles available!
  HDLC32_RX_ISR_ERR: no particles available! HDLC32_RX_ISR_ERR: no particles available!

  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=64689BC0, count=0
  -Traceback= 0x6100C244 0x604B9F4C 0x60955894 0x60959690 0x60AFCE14 0x60AFF7E4

  %ALIGN-1-FATAL: Illegal access to a low address addr=0x0, pc=0x609560C0 ,
  ra=0x609596BC , sp=0x6476BBF8

  %ALIGN-1-FATAL: Illegal access to a low address addr=0x0, pc=0x609560C0 ,
  ra=0x609596BC , sp=0x6476BBF8

  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x609560C0 -Traceback=
  0x609560C0 0x609596BC 0x60AFCE14 0x60AFF7E4
  ```

  Conditions: This symptom is observed on a Cisco router when you enter the **channel group** command to create a serial interface on an NM-HD or NM-HDV2 network module or on an onboard controller of an Integrated Services Router (ISR) such as a Cisco 2800 series or Cisco 3800 series.

  Workaround: There is no workaround.

- CSCsa98520

  Symptoms: A router crashes when the size of the IPv6 hash table is set to 2039, 4093, or 8191.

  Conditions: This symptom is observed on a Cisco router when the size of the IPv6 hash table is set before other inspection attributes are configured.

Workaround: Set the size of the hash table after the IPv6 inspect rule is defined. For example, enter the following sequence of commands:

```
ipv6 inspect name ipv6inspect tcp
int fa0/0
ipv6 inspect ipv6inspect in
exit
ipv6 inspect hashtable-size {2039 or 4093 or 8191 } ==> now no core dump occurs.
```

- CSCsa99446

  Symptoms: A VoIP call is prematurely disconnected during a call hold period.

  Conditions: This symptom is observed on a Cisco platform that attempts to match the rotary dial peers.

  Workaround: There is no workaround.

- CSCsb03192

  Symptoms: When you change the NHRP mapping configuration, an incorrect NHRP cache entry and incorrect crypto socket entry may occur.

  Conditions: This symptom is observed when you change the NHRP static mapping entry by entering the **ip nhrp map** command. The NHRP cache entry is not updated with the new mappings, causing the crypto socket entry to be incorrect.

  Workaround: To change the NHRP static mapping configuration, remove the NHRP mapping entry by entering the **no ip nhrp map** command and then add the NHRP mapping entry by entering the **ip nhrp map** command.

- CSCsb04135

  Symptoms: About 80-percent of the packets that enter though an FE interface and leave through an ATM egress interface are dropped.

  Conditions: This symptom is observed on a Cisco IAD2430 when fast-switching or CEF-switching is enabled.

  Workaround: There is no workaround.

- CSCsb04721

  Symptoms: When the Any Transport over MPLS (AToM) feature is enabled on a router, AToM virtual circuits to a peer may not be re-established after an interface flap or after being reconfigured, because the required targeted Label Distribution Protocol (LDP) session is not re-established.

  Conditions: This symptom is observed when LDP is not configured on any interfaces via the **mpls ip** interface configuration command, which is typically the case when MPLS Traffic Engineering (TE) tunnels are used to transport AToM traffic between endpoints and when the **mpls ip** interface configuration command is not enabled on any TE tunnels.

  The symptom occurs in Cisco IOS software releases that include the fix for caveat CSCec69982 when any form of one of the following commands is configured on the router and appears in the running configuration:

  ```
  mpls ldp explicit-null
  mpls ldp advertise-labels
  mpls ldp session protection
  mpls ldp password fallback
  mpls ldp password option
  mpls ldp password required
  ```

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec69982.

Workaround: Enter the **mpls ip** command on a TE tunnel interface or temporarily on a physical interface to force LDP to be re-established.

- CSCsb04965

  A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

  Cisco is 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-20060920-docsis.shtml.

- CSCsb05381

  Symptoms: MGCP BRI backhaul calls fail, and debugs for the call failure show the following information:

  ```
  400 67 Voice call setup failed-Incoming-Outgoing call collision
  //-1/xxxxxxxxxxxx/VTSP:():-1:-1:-1/vtsp_call_setup_request:
  CALL_ERROR_INFORMATIONAL; Glare Occurred B-Channel=1, Call Id=9
  ```

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(1).

  Workaround: There is no workaround.

- CSCsb05521

  Symptoms: A voice gateway may generate a spurious memory access while testing IEC.

  Conditions: This symptom is observed on a voice gateway that runs Cisco IOS interim Release 12.4(2.3) or interim Release 12.4(2.2)T when some IVR verbs that are also used for fax scenarios are executed. The symptom is platform-independent and related to the timing of a bridge drop and not to the type of traffic.

  Workaround: There is no workaround.

- CSCsb06330

  Symptoms: A router may crash when you make basic IPIPGW fax calls.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T6.

  Workaround: There is no workaround.

- CSCsb06649

  Symptoms: A Cisco 3725 that is configured as an H.323 gateway does not provide three beeps for a tone-on-hold. Instead, it generates the no-circuit tone.

  Conditions: This symptom is observed on a Cisco 3725 that runs Cisco IOS Release 12.3(14)T2 and that is not configured for Music on Hold.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(11)T5.

- CSCsb06658

  A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

  Cisco is 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-20060920-docsis.shtml.

- CSCsb08192

  Symptoms: A Cisco 3800 series may not drop unicast Ethernet frames that are not destined for its MAC address.

  Conditions: This symptom is observed on a Cisco 3800 series that runs Cisco IOS Release 12.3(11)T5 or an earlier release or Release 12.3(14)T1 or an earlier release and that has subinterfaces that are configured for HSRP.

  Workaround: Enter the **standby use-bia** command on the main interface.

- CSCsb08428

  Symptoms: A router may crash when a VPN tunnel is established.

  Conditions: This symptom is observed on a Cisco router when an interface has both IPSec and the **ip verify unicast reachable-via** command enabled and when a hardware encryption engine is used for IPSec.

  Workaround: Remove the **ip verify unicast reachable-via** command from the interface.

- 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.

- 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

- CSCsb14481

  Symptoms: Active voice and fax calls may stop unexpectedly on a gateway, that is, either the call may drop or two-way audio may stop.

  Conditions: This symptom is observed when a DSP recovery algorithm on the gateway is started in response to a DSMP-3-DSP_TIMEOUT error condition. The timeout may occur on one of the channels of the DSP, but the reset algorithm impacts other calls on other channels that are active on the same DSP.

  Network modules with 549 and 5421 DSPs such as the NM-HDV and AIM-VOICE network modules are reset when this timeout occurs, causing other active voice and fax calls on other channels of the same DSP to be reset. Network modules that use 5510 DSPs such as the NM-HDV2 network module do not seem to be reset when this timeout occurs during statistics collection.

  To verify which DSP is currently in use on a gateway, enter the **show voice dsp** EXEC command.

  Workaround: Disable the DSP recovery algorithm by entering the **test dsp recovery disable** command. However, use this command with caution because disabling the auto-recovery mechanism prevents voice and fax calls from functioning properly when a DSP enters a valid non-responding state.

  Further Problem Description: This fix for this caveat suppresses the resetting of the DSP when the timeout occurs under a statistics collection state as shown in the sample output below where the state is equal to S_DSMP_COLLECTING_STATS:

  ```
  %DSMP-3-DSP_TIMEOUT: DSP timeout on DSP 1/5:4: event 0x6, DSMP timed out, while
  waiting for statistics from the DSP. DSMP State = S_DSMP_COLLECTING_STATS
  ```

  The timeout may occur when an internal software error causes some invalid statistics to be polled, leading to the timeout. As an example, see caveat CSCsa72951.

- CSCsb16024

  Symptoms: There is no voice path when you make a full-consult transfer.

  Conditions: This symptom is observed on a Cisco 3800 series that runs Cisco IOS interim Release 12.4(2.8), functions as a gateway, and that is configured for Survivable Remote Site Telephony (SRST).

  Workaround: There is no workaround. Note that the symptom does not occur in interim Releases 12.4(2.1) and 12.4(2.2).

- CSCsb16695

  Symptoms: A Cisco IGX 8400 series URM does not boot and generates a traceback message.

  Conditions: This symptom is observed on a Cisco IGX 8400 series URM that runs Cisco IOS interim Release 12.4(1.8).

  Workaround: There is no workaround.

  Further Problem Description: To enable the router to enter the ROMmon mode, continuously enter the **send break** command from the console and then boot the router by using the Cisco IOS software image in bootflash. When the router is accessible, you can configure the router to boot from bootflash by entering the **cnfrtrparm** *urm-slot* **1 2** and **resetcd** commands.

- CSCsb24007

  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

- CSCuk56944

  Symptoms: A router crashes when you remove X.25 WAN encapsulation from an interface that is configured for TCP header compression.

  Conditions: This symptom is observed on a Cisco router that run Cisco IOS interim Release 12.4(0.4).

  Workaround: Remove TCP header compression before you change the WAN encapsulation, as in the following example:

```
router(config)#int ser3/0
router(config-if)#no x25 map compressedtcp 10.10.10.11 170091
router(config-if)#no ip add
router(config-if)#no ip address
router(config-if)#encap frame
router(config-if)#encap frame-relay
```

TCP/IP Host-Mode Services

- CSCsa62111

  Symptoms: Packets may be stuck in the input queue of a Cisco 7200 series.

  Conditions: This symptom is observed on a Cisco 7200 series that is running Cisco IOS interim Release 12.3(12.10) and that is configured with an NPE-G1.

  Workaround: Reload the router to clear the input queue or increase the input queue beyond the default limit of 75 via the **hold-queue** *length* command.

Wide-Area Networking

- CSCea75722

  Symptoms: A Cisco IOS voice gateway may fail to receive a call from the public switched telephone network (PSTN) on its PRI port.

  Conditions: This symptom is observed on a Cisco 2651XM that runs Cisco IOS Release 12.2(13)T3 or Release 12.3 and that functions as a voice gateway when it does not send a Q.931 Call Proceeding message upon receiving the call.

  Workaround: There is no workaround.

- CSCef58201

  Symptoms: The CEF-Dialer feature fails to add an adjacency for a virtual-access1 CEF interface because the IP route is installed after the feature attempts to add the adjacency.

  Conditions: This symptom is observed during a test on a Cisco router that runs Cisco IOS Release 12.3 or interim Release 12.3(10.3)T.

  Workaround: Configure a static host entry for the neighbor in the routing table, pointing to the Dialer interface:

  ip route *prefix mask* **255.255.255.255 Dialer1**

  For the *prefix mask* argument, enter the IP address of the neighbor.

- CSCeg03958

  Symptoms: A router may crash while performing an SNMP walk on VPDN-related MIB Objects. SNMP get and set operations function fine.

  Conditions: This symptom is observed on a Cisco router that is configured with MLP interfaces.

  Workaround: Reload the router and do not perform an SNMP walk. Instead use get operations.

- CSCeg15248

  Symptoms: Uninteresting traffic is blocked even after the link is up.

  Conditions: This symptom is observed only on an interface that is configured for dialer DTR.

  Workaround: There is no workaround.

- CSCeg22171

  Symptoms: Calls fail to connect when they are switched from the primary D channel to the backup D channel.

  Conditions: This symptom is observed when you either unplug the cable or shut down the controller of the primary D channel.

  Workaround: There is no workaround.

- CSCeg22533

  Symptoms: A signal-only call fails when an INVALID message is generated because a B-channel IDB is not found.

  Conditions: This symptom is observed when ISDN PRI QSIG Voice Signaling is configured.

  Workaround: There is no workaround.

- CSCeg42148

  Symptoms: Attempts to change a B-channel service state by entering the **isdn service nfas-int** *number* **b_channel** *number* {**state** {**0** | **1** | **2**} [**hard** | **immediate** | **soft**]} command appear to succeed but the service state does not change.

  Conditions: This symptom is observed when a voice application uses a B-channel. The output of the **show isdn service detail** command shows a locale of ISDN_NEAR_END_APP.

  Workaround: There is no workaround.

- CSCeg55098

  Symptoms: When an ISDN switch deactivates layer 2, a router immediately activates layer 2. The output of the **debug isdn q921** command shows that the router activates layer 2 within 6 milliseconds:

  ```
  ISDN BR0 Q921: User RX <- DISCp sapi=0 tei=65
  ```

```
....
BR0 Q921: User TX -> UAf sapi=0 tei=65
```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T2 and that is configured with a BRI. Note that the symptom does not occur in Release 12.3(11)T.

Workaround: There is no workaround. However, to prevent the consecutive line up/down messages from being generated, enter the following interface configuration commands:

interface *bri number*
no logging event link-status

- CSCeg61278

  Symptoms: A router that is configured for ISDN may reload because of a SegV exception.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(12) only when the BRI-NET3 switch type is configured and when the BRI interface emulates the network side. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeg74644

  Symptoms: A Cisco 3660 that is configured for PPPoE relay may reload.

  Conditions: This symptom is observed on a Cisco 3660 that runs Cisco IOS Release 12.3(7)T7.

  Workaround: There is no workaround.

- CSCeg82698

  Symptoms: PPTP tunnels do not come up.

  Conditions: This symptom is observed when VPDN is configured.

  Workaround: There is no workaround.

- CSCeg88174

  Symptoms: Drops occur in a class in which the throughput does not oversubscribe the allocated bandwidth for the class.

  Conditions: This symptom is observed when multilink Frame Relay is configured along with generic traffic shaping or Frame Relay traffic shaping and when several class maps are configured.

  When one class map starts dropping packets because the throughput is greater than the allocated bandwidth (which is normal behavior), drops may also occur in another class map even though this class map is not oversubscribed. The root cause of this symptom is that the bundle is oversubscribed and tx rings are building up, causing excessive misordering that the receiver cannot handle.

  Workaround: Configure a fancy queue on the bundle interface through which the traffic is sent.

- CSCeg88737

  Symptoms: A Cisco 7200 series may crash because of memory corruption.

  Conditions: This symptom is observed when the router has an input QoS configuration on an MFR interface.

  Workaround: There is no workaround.

- CSCeg90765

  Symptoms: Data traffic that is received on a Multilink PPP over ATM (MLPoA) connection may be dropped.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for MLPoA and CEF switching.

Workaround: Disable CEF switching.

- CSCeh06916

  Symptoms: A Cisco router crashes when PVCs are deleted while the **show pppoe session** or **show vpdn** command is entered.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for PPP over Ethernet (PPPoE) when there are two concurrent Telnet sessions. PVCs are deleted via one Telnet session while the **show pppoe session** or **show vpdn** command is entered via the other Telnet session. The symptom is platform-independent.

  Workaround: Do not delete PVCs via one session and enter the **show pppoe session** or **show vpdn** command via another session at the same time.

- CSCeh11771

  Symptoms: On a leased line (non-dialup) serial connection that is configured for PPP encapsulation, the line protocol may not come back up when the connection is reset. The PPP LCP remains in the closed state, even though the link is up physically.

  Conditions: This symptom is observed when an active PPP session is reset and when the underlying link is not simultaneously reset, that is, when PPP goes down but when the link does not go down physically. This situation would occur, for example, when a PPP session is terminated because of keepalive failures.

  Workaround: There is no workaround.

- CSCeh11994

  Symptoms: A reply of an LNS to a LAC may be delayed.

  Conditions: This symptom is observed on a Cisco router that is configured as an LNS that has several tunnels to different LACs.

  Workaround: There is no workaround.

- CSCeh18018

  Symptoms: The asynchronous resources on a NAS may remain active after a VPDN setup because the LAC does not close the L2TP session on receipt of the L2TP Call Disconnect Notification (CDN) from the LNS.

  Conditions: This symptom is observed on a NAS that is configured with digital modems when the L2TP session is abnormally aborted, for example, when the L2TP session is aborted before the LNS sends an LCP termination request to the dialin user.

  Workaround: Manually free the asynchronous resources on the NAS by entering the **clear line** *line-number* command or ask the remote dialin user to disconnect the modem.

- CSCeh22021

  Symptoms: When you attempt to establish a PPP session over an ATM interface, the following error message is generated and the session is not established:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=440A7FA0, count=0"
  ```

  Conditions: This symptom is observed on a Cisco MGX 8800 series RPM-XF that runs Cisco IOS Release 12.4 when PPP over ATM is configured. However, the symptom may also occur on another Cisco router (from the Cisco 2600 series through the Cisco 7300 series) that runs Release 12.4.

  Workaround: There is no workaround.

- CSCeh25440

  Symptoms: InvARP packets on multiple MFR bundle interfaces may be dropped, causing traffic to fail after you have reloaded microcode onto a line card that processes a high load of traffic over many PVCs on MFR interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when 42 MFR bundles are configured over 336 full T1s and when egress MQC is configured on the 42 MFR bundle interfaces. However, the symptom is not platform- and release-specific.

  Workaround: There is no workaround.

- CSCeh32353

  Symptoms: An LNS intermittently routes packets to an incorrect interface in the process-switching path, preventing some applications from working properly. These applications such as ARP, CBAC, and NAT depend on the first packet to go to process-switching for their initialization operation. Consequently, this situation may affect user connectivity to the Internet.

  Conditions: This symptom is observed when the next-hop ISP router is connected via static routes and when there is no ARP entry on the LNS.

  Workaround: There is no workaround.

- CSCeh33185

  Symptoms: A POS interface on a VIP4-80 that is configured for PPP goes down and remains down.

  Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0S only when PPP receives an LCP PROTOCOL REJECT message for PAP or CHAP. The symptom may also occur in other releases.

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

- CSCeh34067

  Symptoms: The route processor of a Cisco 7613 may crash when stress traffic is processed on all WAN links of FlexWANs in which channelized port adapters are installed and when interfaces of the channelized port adapters flap.

  Conditions: This symptom is observed when the channelized port adapters are configured for MFR. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCeh41079

  Symptoms: Packets get CEF switched even though the interface is configured for dCEF.

  Conditions: This symptom is observed on a Cisco 7500 series router when the dialer legacy/profile is configured.

  Workaround: There is no workaround.

- CSCeh48987

  Symptoms: The CEF-Dialer feature fails to add an adjacency for a Virtual-Access1 CEF interface.

  Conditions: This symptom is observed during a test on a Cisco router that runs Cisco IOS interim Release 12.3(14.10).

  Workaround: There is no workaround.

- CSCeh53438

  Symptoms: The **ip idle-group** command does not function when it is downloaded from a RADIUS server.

  Conditions: This symptom is observed when the **ip idle-group** command is configured in the user profile on the RADIUS server.

  Workaround: Configure the **ip idle-group** command locally on a virtual template.

- CSCeh56780

  Symptoms: A router may crash when you enter the **no interface atm** command.

  Conditions: This symptom is observed on a Cisco router while PPPoE sessions come up.

  Workaround: First enter the **shutdown** command on the interface before you enter the **no interface atm** command.

- CSCeh59311

  Symptoms: None of the digits in INFO messages are passed to an ISDN switch.

  Conditions: This symptom is observed on a Cisco 1760 that runs Cisco IOS Release 12.3(11) or Release 12.3(11)T4 when overlap is configured and when the setup acknowledgement arrives late from the terminating switch after some of the INFO messages have already been received from the OGW. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCeh62257

  Symptoms: PPP does not establish new sessions.

  Conditions: This symptom is observed on a Cisco router that is configured with full virtual-access interfaces when a PPP leak occurs.

  Workaround: Reload the router and configure virtual-access subinterfaces instead of full virtual-access interfaces.

- CSCeh80705

  Symptoms: A redirected VoIP call may fail.

  Conditions: This symptom is observed when a Cisco gateway sends redirected number information in the redirection IE but not in the ISDN Facility divertingLegInformation2.

  Workaround: There is no workaround.

- CSCei00766

  Symptoms: A router may crash when the encapsulation is set to PPP and removed repeatedly.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.4 and that is configured for PPP Link Control Protocol (LCP).

  Workaround: There is no workaround.

- CSCin53003

  Symptoms: A platform that is configured for ISDN may crash when you make a T.38 call.

  Conditions: This symptom is observed only when you restart a B channel.

  Workaround: Do not restart the B channel.

- CSCin83822

  Symptoms: When a bus or CyBus error occurs, the following error messages may be generated in the log of a VIP and the VIP may crash:

```
IOBUS Error Interrupt Status register 0x4 Address/Command Strobe Timeout
IOBUS Error Address High 0x1C01 IOBUS Error Address Low 0xC
```

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

Workaround: There is no workaround.

- CSCin86951

  Symptoms: An LNS router crashes on establishing a large number of PPPoA L2TP sessions.

  Conditions: This symptom is observed only when you establish sessions at a high rate. When you attempt to establish 8000 sessions, the router crashes shortly after 5000 sessions are established.

  Workaround: Establish sessions at a low rate.

- CSCin88952

  Symptoms: When a dialer interface is configured for legacy Dial-On-Demand Routing (DDR) for calling, a ping does not succeed, and a call is not set up.

  Conditions: This symptom is observed on a Cisco platform that is configured for legacy DDR.

  Workaround: Configure the dialer map on a hardware interface such as a to enable the call to be set up.

- CSCsa52807

  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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa54870

  Symptoms: A pure TDM call that originates from a PRI side and that is destined for a BRI side fails during the call setup.

  Conditions: This symptom is observed only when the ISDN switch type is NI2 in the following topology:

  ```
  [phone]----[PRI-OGW]----[PRI-BRI-GW]----[BRI-TGW]----[phone]
  ```

Workaround: Configure another switch type than NI on the BRI.

Alternate Workaround: Configure explicitly the **isdn point-to-point-setup** command on the BRI NI network-side.

- CSCsa66756

  Symptoms: The B channel on an NFAS “none” group member may hang with its channel state set to PROPOSED, which you can see in the output of the **show isdn service** command.

  Conditions: This symptom is observed when the first activity on an NFAS “none” member is an outgoing call. After the first incoming or outgoing call, the symptom does no longer occur.

  Workaround: There is no workaround.

- CSCsa71228

  Symptoms: Callback does not occur.

  Conditions: This symptom is observed when the **dialer map** command is configured on a dialer interface for a rotary group configuration.

  Workaround: Enter the **dialer string** command in the dialer profile configuration.

- CSCsa73099

  Symptoms: A router may run out of free memory in the processor pool as a consequence of a memory leak in the ISDN process. The output of the **show memory** command shows that the blocks of memory that are not freed are allocated for “AAA Event Data” or “AAA Event.”

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that includes the fixes for CSCef87435 and CSCef57881 and that is configured with ISDN interfaces that are active.

  Workaround: There is no workaround.

- CSCsa73905

  Symptoms: The L2TP management daemon process may leak memory if the parsing of some L2TP control messages fails.

  Conditions: This symptom is observed on a Cisco router that is configured or VPDN L2TP tunnels when PPPoE sessions were brought up and down after a period of time.

  Workaround: There is no workaround.

- CSCsa78067

  Symptoms: A Cisco 5400HPX may crash when conditional debugging runs.

  Conditions: This symptom is observed on a Cisco 5400HPX that runs Cisco IOS Release 12.3(11)T3 when ISDN globally unique identifier (GUID) is configured.

  Workaround: There is no workaround.

- CSCsa78148

  Symptoms: A Cisco router that functions as an L2TP Network Server (LNS) may drop sessions when multilink is enabled and negotiated on a forwarded inbound VPDN session.

  Conditions: This symptom is observed when LCP renegotiation of proxy negotiations is disabled (which is the default) and when the multilink Endpoint Discriminator option that is advertised by the LAC does not match the Endpoint Discriminator on the LNS.

  Workaround: Enable the LNS to renegotiate LCP when necessary by entering the **lcp renegotiation on-mismatch** VPDN group configuration command.

Alternate Workaround: Avoid the need to renegotiate by entering the **ppp chap hostname** or **ppp multilink endpoint** command to configure matching Endpoint Discriminators on the LAC and LNS.

Warning: Technically, the current behavior of the Cisco IOS software is correct. An LNS should not accept the results of a LAC proxy negotiation when the LAC negotiates values that do not accurately represent the LNS. A platform must be configured to either enable the LNS to renegotiate when necessary, or (if it is desired to avoid such renegotiations, which may be necessary to get around problematic client implementations) enable the LAC to negotiate adequately as a substitute for the LNS.

The fix for CSCsa78148 deliberately introduces the behavior that a mismatched multilink Endpoint Discriminator is ignored when the LNS is configured to terminate connections on mismatched conditions. This behavior is introduced to prevent the termination of a connection for a condition that is harmless for the majority of VPDN users. From a technical standpoint, this behavior is improper because it means that the VPDN clients have an invalid notion of the identity of the peer. This situation may pose problems for clients who have more than one multilink-capable link active at a time because the invalid Endpoint Discriminators may prevent links from being properly bundled at the client end. In such circumstances, enabling LCP renegotiation or ensuring that the LAC and LNS agree on negotiation parameters is the only valid option.

- CSCsa81268

  Symptoms: A Cisco AS5850 may reload with a software forced crash.

  Conditions: This symptom occurs when configuring the **isdn ie oli** interface configuration command.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(1c)

Cisco IOS Release 12.4(1c) is a rebuild release for Cisco IOS Release 12.4(1). The caveats in this section are resolved in Cisco IOS Release 12.4(1c) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCei21133

  Symptoms: A router reloads because of a watchdog timeout when you perform an snmpwalk.

  Conditions: This symptom is observed on a Cisco 7200 series but may be platform-independent. The traceback stack decode points to an EIGRP function although EIGRP is not configured on the router.

  Possible Workaround: Configure a dummy EIGRP router process, for example one for which the network covers only a loopback interface, so that the snmpwalk does not cause the router to crash.

- 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.

- CSCsb32141

  Symptoms: A router that is configured for Resource Reservation Protocol (RSVP) generates the following error messages on the console and then crashes:

  ```
  %LINK-0-REENTER: Fatal reentrancy, level=3, intfc=FastEthernet0/1
  -Process= "RSVP", ipl= 3, pid= 251
  %SYS-6-STACKLOW: Stack for process RSVP running low, 0/24000
  ```

  Conditions: This symptom is observed when the **ip rsvp bandwidth** and **service-policy output** commands are configured on the same interface and when the policy map for the service policy is configured with the **fair-queue** command.

  Workaround: Enter the **ip rsvp resource-provider** *none* command on the interface.

  Alternate Workaround: Enter the **ip rsvp bandwidth** *value* command and ensure that the *value* argument is equal to the value that is displayed on the "Available Bandwidth" line in the output of the **show interface** *interface* command plus the value that is shown in the "allocated" column in the output of the **show ip rsvp interface** command.

Miscellaneous

- CSCed94829

  Multiple Cisco products contain vulnerabilities in the processing of IPSec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for IPSec and can be repeatedly exploited to produce a denial of service.

  Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

  This advisory is posted at

  http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.shtml.

- CSCef84174

  Symptoms: PPP forwarding may fail between two virtual access interfaces.

  Conditions: This symptom is observed on a Cisco AS5850 but is not platform-dependent.

  Workaround: Disable PPP multilink on the asynchronous interfaces.

- CSCeh09198

  Symptoms: A Cisco gateway that has the garbage detector (a tool that is used for debugging memory leaks) enabled may hang indefinitely.

  Conditions: This symptom is observed when you enter the garbage detector-related **show memory debug leaks** command or **show memory debug incremental leaks** command.

  Workaround: There is no workaround.

- CSCeh47169

  Symptoms: A Cisco router may reload because of I/O memory corruption when you use Telnet, reverse Telnet, rsh, or other vty-based applications, for example, a vty-based application to access a service module.

  Conditions: This symptom is observed on a Cisco 2851, Cisco 3745, and Cisco 3845 that contain the fix for caveat CSCef84400.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef84400. 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.

- CSCeh61467

  This caveat consists of the two symptoms, two conditions, and two workarounds:

  Symptom 1: After you have disabled MVPN on a VRF interface, the CPU use for the PIM process increases to 99 or 100 percent and remains at that level.

  Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases.

  Workaround 1: Before you disable MVPN on the VRF interface, enable and then disable multicast routing by entering the **ip multicast-routing vrf** *vrf-name* global configuration command followed by the **no ip multicast-routing vrf** *vrf-name* global configuration command.

  Symptom 2: A router that functions under stress and that is configured with a VRF interface may crash when an MDT group is removed from a remote PE router.

  Condition 2: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SX, or a release that is based on these releases, and occurs only when there are frequent link flaps or other multicast topology changes that affect the VRF interface.

  Workaround 2: There is no workaround.

- CSCeh73049

  Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at

  http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

- CSCei02275

  Symptoms: A Cisco router may reload when removing a Frame Relay map from a dial interface.

  Conditions: This symptom occurs when a dial (ISDN) interface is configured for Frame Relay encapsulation with a map that includes IP Header Compression.

  Workaround: There is no workaround.

- CSCei08458

  Symptoms: The FIB may be disabled or the output interface may be stuck on an A3 ATM port adapter.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dLFIoATM.

  Workaround: Reload the microcode or perform an OIR to recover the A3 ATM port adapter.

- CSCin79691

  Symptoms: QoS information disappears from a FlexWAN module or VIP that is configured with a distributed MFR interface.

  Conditions: This symptom is observed after the FlexWAN module or VIP resets or after the interface flaps.

  Workaround: Remove the service policy from the interface and reapply it to the interface.

- CSCin91381

  Symptoms: A VIP card having a dMLFR configuration on a Cisco 7500 series router may crash on entering the **microcode reload** command in the global configuration mode.

  Conditions: This symptom has been observed on a Cisco 7500 series router with a VIP card having a dMLFR configuration when traffic is flowing at that point of time.

  Workaround: There is no workaround.

- CSCsa53334

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml.

- CSCsa68001

  Symptoms: All incoming packets on a Frame Relay Link have the DE bit set.

  Conditions: This symptom is observed on a Cisco 2811 that runs Cisco IOS Release 12.3 or Release 12.3(11)T2 under normal traffic conditions.

  Workaround: There is no workaround. Note that the symptom does not occur on a Cisco 1760 that runs Release 12.3(10).

- CSCsa86291

  Symptoms: Packets that enter on an interface that has the **ssg direction downlink** command enabled are not translated even though the **ip nat inside** is enabled.

  Conditions: This symptom is observed on a Cisco router that is configured for SSG with the TP, TT, or TX type of service and that runs Cisco IOS Release 12.3(11)T4 or Release 12.3(14)T. The symptom may also occur in Release 12.3 but does not occur in Release 12.3(11)T3.

  Note that when you disable the **ssg direction downlink** command on the interface, NAT works fine.

  Workaround: There is no workaround.

- CSCsa86390

  Symptoms: A router generates an ALIGN-3-TRACE traceback and a DSPDUMP in its log, and the output of the **show align** command shows that the spurious access counter is not zero.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 2800 series when an error message is generated during stress calls.

  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.

- CSCsb33129

  Symptoms: A router may reload unexpectedly when the SSG queue for RADIUS requests that are in the waiting state becomes too large.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(14)T1 or Release 12.4(1a) and that is configured for SSG. When there is a large number of RADIUS requests or a connectivity problem between SSG and the RADIUS server, the SSG queue for RADIUS requests that are in the waiting state may become too large.

  Workaround: There is no workaround.

- CSCsb65056

  Symptoms: A PPP connection may remain active after the idle-timer zeroes out. This situation may affect other services that rely on the termination of the PPP connection. Also, an incorrect redirection may occur.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSG when the host object is disconnected but the PPP connection remains active.

  Workaround: There is no workaround.

  Further Problem Description: After the host idle-timeout/user idle-timeout in the output of the related virtual access interface, you can troubleshoot the situation through the **debug ssg events** command.

- CSCsb72138

  Symptoms: A Foreign Exchange Station (FXS) port may lock up after having functioned fine for a long time.

  Conditions: This symptom is observed on a Cisco 2821 that runs Cisco IOS Release 12.3(11)T5. This symptom typically occurs when fax lines are configured on the FXS port.

  Workaround: There is no workaround.

- CSCsc09246

  Symptoms: The following commands used for detecting memory leaks would crash the router which uses external memory such as the RPM-XF platforms.

show memory debug leaks show memory debug leaks chunks show memory debug leaks largest show memory debug leaks summary

Conditions: This symptom has been observed on the RPM-XF cards using Cisco IOS interim Release 12.4(4.6).

Workaround: There is no workaround.

Wide-Area Networking

- CSCei11919

  Symptoms: A dialed circuit that carries a PPP connection over a tunnel between an LNS and a LAC is not dropped when the tunnel is reset.

  Conditions: This symptom is observed when you enter the **clear vpdn all** command, when the LNS reloads, when the IP link between the LSN and LAC is disrupted, or when any other event occurs that causes the tunnel to be reset.

  Workaround: There is no workaround.

- CSCej45061

  Symptoms: Attempts to remove a PRI group fail.

  Conditions: This symptom is observed when an NFAS group has group number 0 and when you attempt to remove a FAS PRI group.

  Workaround: Shut down the NFAS group before you remove the FAS PRI group.

- CSCsa55747

  Symptoms: The RADIUS L2TP-specific disconnect code value for the Ascend-Disconnect-Cause RADIUS attribute (195) is incorrectly generated as 607 instead of 605.

  Conditions: This symptom is observed when an L2TP tunnel setup failure occurs between a LAC and an LNS.

  Workaround: There is no workaround.

- CSCsa66756

  Symptoms: The B channel on an NFAS "none" group member may hang with its channel state set to PROPOSED, which you can see in the output of the **show isdn service** command.

  Conditions: This symptom is observed when the first activity on an NFAS "none" member is an outgoing call. After the first incoming or outgoing call, the symptom does no longer occur.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(1b)

Cisco IOS Release 12.4(1b) is a rebuild release for Cisco IOS Release 12.4(1). The caveats in this section are resolved in Cisco IOS Release 12.4(1b) but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

- CSCef00114

  Symptoms: A router reloads unexpectedly when a tunnel password is downloaded via a RADIUS server.

  Conditions: This symptom is observed when a tunnel password is configured in the RADIUS domain profile that is used to establish the tunnel and when the tunnel password string consists of more than 64 characters.

  Workaround: Configure a tunnel password string that consists of less than 64 characters.

- CSCeh04755

  Symptoms: When you reload a router by entering the **reload** command, the router may unexpectedly enter the ROMmon mode and generate the following error message:

  ```
  %SYS-5-RELOAD: Reload requested by console.
  Reload Reason:Reload command.
  monitor: command "boot" aborted due to user interrupt
  rommon 1 >
  ```

  Conditions: This symptom is observed only on a Cisco 7200 that is configured with an NPE-G1, and on UBR7246VXR with UBR-NPE-G1

  Workaround: Enter the **confreg 0x2002** command.

- CSCeh64791

  Symptoms: A memory leak may occur when you delete a RADIUS server group.

  Conditions: This symptom is observed when the server is configured with a key.

  Workaround: There is no workaround.

- CSCeh65692

  Symptoms: Spurious memory access errors and tracebacks may be generated on a Cisco AS5800.

  Condition: This symptom is observed on a Cisco AS5800 that processes TCPclear calls.

  Workaround: There is no workaround.

- CSCin81985

  Symptoms: Although a RADIUS server is up and running, a router may not contact the RADIUS server during login authentication.

  Conditions: This symptom is observed when the RADIUS server is declared dead and then, after an accounting-on record is sent, changes to the up state.

  Workaround: Configure local authentication as a backup by entering the **aaa authentication login default group radius local** command and a local user name and password.

- CSCin90842

  Symptoms: Memory allocations fail on the gateway though there is enough free memory. If this failure happens in ISDN, the gateway crashes subsequently.

  Conditions: This symptom has been observed when the **H323 aaa accounting** command is enabled.

  Workaround: There is no workaround.

  Further Problem Description: Memory allocations for a block of 3k bytes fail with memory fragmentation as the cause. When this failure occurs, there is approximately 20MB of free memory on a gateway with 220MB of processor memory.

- CSCsb03401

  Symptoms: You cannot open a specific port on a Cisco IOS IP SLA responder.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T1 when you attempt to open a specific port on the responder instead of using normal control protocol. The symptom may also occur in Release 12.4 or Release 12.4T.

  Workaround: Use normal control protocol.

- CSCsb27960

  Symptoms: When the local method is used at the beginning of a PPP authentication method list and when a user does not exist in the local database, failover to the next method in the method list does not occur. This situation prevents users that are listed in the database of a RADIUS or TACACS+ server from being authenticated.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA.

  Workaround: Temporarily remove the local method from the beginning of the method list.

- CSCsb49500

  Symptoms: SNMP traps do not function, preventing an SNMP notification view from being properly associated with a default group that was created via the **snmp-server host** command.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(2)T.

  Workaround: Enter the **show snmp view** command to obtain the SNMP notification view and then apply this view to the default group that was created via the **snmp-server host** command.

Interfaces and Bridging

- CSCei08289

  Symptoms: The transmit rate is higher than the configured committed information rate (CIR), causing the network to drop frames.

  Conditions: This symptom is observed only when traffic is process-switched and when software payload compression and header compression are configured.

  Workaround: Enable either CEF or fast-switching. If process-switching must be used, add a compression adaptor and configure FRF9 data compression instead of packet-by-packet payload compression. You can enable FRF9 data compression in the following ways:

  – On a point-to-point interface, enter the following command in interface configuration mode:

```
frame-relay payload-compression frf9 stac
```

  – On a multipoint interface, enter the following command in interface configuration mode:

  frame-relay map ip *ip-address dlci* **payload-compression frf9 stac**

Further Problem Description: We do not recommend process-switching in combination with software payload compression because it is not possible to provide latency guarantees.

- CSCin88048

  Symptoms: The protocol does not come up when channelized T3 is changed to unchannelized.

  Conditions: This symptom has been observed when a channelized T3 is changed to the unchannelized mode.

  Workaround: Reconfigure or reboot the router.

IP Routing Protocols

- CSCef21601

  Symptoms: Calls may not complete because ResvConfirm messages are dropped. You can enter the **debug ip rsvp messages** command to track RSVP messages as they traverse routers.

  Conditions: This symptom is observed when RSVP is configured for call admission control in a network with routers that do not have RSVP and a proxy ARP enabled. The symptom occurs because the RSVP-capable hop that sends the ResvConfirm messages uses the next RSVP-capable hop as the next IP hop for the packets and does not have the MAC address that is needed to encapsulate the IP packets for this next IP hop.

  Workaround: Configure a static ARP entry that enables the router to properly encapsulate the packet by entering the **arp** *ip-address hardware-address* **arpa** command. The *ip-address* argument is the address of the next hop (that is visible via the RSVP debugs) for the ResvConfirm messages and the *hardware-address* argument is the MAC address of the interface of the next IP hop through which the ResvConfirm messages should be routed.

- CSCeh15639

  Symptoms: A Cisco router may crash when it is reloaded with PIM traffic on the network.

  Conditions: This symptom is observed on a Cisco 7200 series router with multicast enabled but is not platform dependent. Bootup is the most likely place where this will happen, but the router may crash anytime if an interface flap happens at the right time while receiving PIM traffic.

  Workaround: There is no workaround.

- CSCei06089

  Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

- CSCei26899

  Symptoms: When you reset a BGP peer, some prefixes are missing.

  Conditions: This symptom is observed on a Cisco MGX8850 RPM-XF that runs Cisco IOS Release 12.3(11)T. However, the symptom is platform-independent and may also occur in other releases.

  Workaround: There is no workaround.

- CSCsa65155

  Symptoms: IS-IS may not update redistributed BGP network changes.

Conditions: This symptom is observed when the **network** *network-number* command is enabled to introduce connected networks into a BGP topology and when, afterwards, BGP is redistributed into IS-IS. The symptom occurs after one of the interfaces that forms a network connection goes down and comes up again; the network re-enters the BGP topology but is no longer redistributed into IS-IS.

Workaround: There is no workaround.

- CSCsa87473

  Symptoms: A BGP speaker may fail to send all of its prefixes to a neighbor if the neighbor sends a refresh request to the BGP speaker at the same time that the BGP speaker is generating updates to the neighbor. This situation causes the neighbor to miss some prefixes from its BGP table.

  Conditions: This symptom may occur between any pair of BGP speakers.

  A common scenario is that a VPNv4 PE router is reloaded and then fails to learn all prefixes from its route reflector (RR). In this configuration, the symptom occurs when the processing of a VRF configuration causes the PE router to automatically generate a route-refresh request to the RR, while the RR is still generating updates to the PE.

  Workaround: There is no workaround.

- CSCsa94774

  Symptoms: When you enter the **traceroute** command from an IP address that is different from the address in the NAT default configuration, the incoming PAT sends the reply packets to the NAT default address that is defined in the NAT default configuration and not to the original source address from which the **traceroute** command was entered. Note that the outside PAT works fine.

  Conditions: This symptom is platform-independent. NAT overload traffic and other TCP traffic is not affected.

  Workaround: There is no workaround.

- CSCsa98059

  Symptoms: Suboptimal routing occurs in an OSPF configuration or a routing loop occurs between two border routers that redistribute BGP into OSPF.

  Conditions: These symptoms are observed when at least two border routers are connected via eBGP to another autonomous system, receive the same prefix over these connections, and redistribute the prefix into OSPF. Under certain conditions, for example when the eBGP session from the preferred BGP exit point to the eBGP peer flaps, the second router in the local autonomous system becomes the preferred path and redistributes the eBGP route into OSPF. When the eBGP session with the first router comes back up, the LSA should be flushed but this does not occur. This situation may create routing problems on other OSPF routers or, when BGP has a higher administrative distance than OSPF, routing loops between both border routers.

  Workaround: There is no workaround.

- CSCsb07372

  Symptoms: NAT H.323 does not create an entry in the NAT translation table even though debugging shows that NAT processes the packet correctly. This situation causes one-way voice for the called party, preventing them from hearing the calling party.

  Conditions: This symptom is observed only when ICMP error messages are processed by NAT.

  Workaround: There is no workaround.

- CSCsb13988

  Symptoms: A router that is configured for NAT may crash because of a bus error.

Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(9a) but is not platform-specific. The crash occurs while NAT attempts to translate an IP address in an H.323 RAS messages that does not contain an IP address.

Workaround: Disable H.323 RAS in NAT by entering the **no ip nat service ras** command. If you must use H.323 RAS in NAT, there is no workaround.

- CSCsb25662

  Symptoms: When an IP phone that is located at a central site leaves a conference, a one-way voice condition occurs for the remaining two phones in the conference.

  Conditions: This symptom is observed in a Hub-and-Spoke configuration in which both sites perform NAT when a voice conference is created by an IP phone that is located at a central site with two IP phones that are located at a remote site. NAT is configured on the hub and at the remote site, SCCP is the voice signaling protocol, and the conference occurs between the hub and the remote site.

  Workaround: Enter the **clear ip nat translation *** command.

Miscellaneous

- 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.

- CSCef81634

  Symptoms: When you bring up and tear down SSG sessions quickly, a router may crash because of a bus error exception.

  Conditions: This symptom is observed on a Cisco router that is configured for SSG when you use a tool that initializes the interface and quickly brings sessions back up while the old sessions are still being cleared.

  Workaround: There is no workaround.

- CSCeg16631

  Symptoms: When you enter the **distribute-list** *interface* command in a global RIP routing context and the interface that is specified in the command is a VRF interface, the command is rejected with the following error message:

  ```
  % The interface is not in the same VRF as the process
  ```

  Because the **distribute-list** *interface* command is not implemented in the IPv4 VRF address-family, there is no other way to filter networks received in updates via a VRF interface.

  Conditions: This symptom is observed in all Cisco IOS releases that integrate the fix for CSCee32557. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee32557. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: In a configuration that is mentioned above, to filter networks received in updates, enter the **distribute-list** *extended-ACL-reference* command in which the "source-part" of the extended ACL specifies the prefixes and the "destination part" matches on the IP address of the RIP neighbor.

- CSCeg43855

  Symptoms: An encrypting router may send traffic that is locally originated (such as keepalive packets or routing update packets) out of order after the packets have been encrypted. Because of the anti-replay check failure, these packets are dropped on the receiving router.

  Conditions: This symptom is observed when a multipoint GRE (mGRE) and IPSec tunnel is build between two routers.

  Workaround: Turn off packet authentication for the configured IPSec transform.

  Further Problem Description: On a Cisco 7200 series that functions as the receiving router, you can observe the symptom in the output of the **show crypto ipsec sa detail** or **show pas isa interface** command.

- CSCeg52468

  Symptoms: A Cisco router intermittently stops encrypting and forwarding packets, and the following error messages are generated:

  ```
  %VPN_HW-1-PACKET_ERROR slot 0 Packet Encryption/Decryption error, Output
  Authentication error (0x20000000)
  ```

  or

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error,
  Invalid Packet
  ```

  Conditions: This symptom is observed under rare circumstances on a Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series that are configured with an AIM-VPN-BPII, AIM-VPN/EPII, or AIM-VPN/HPII Virtual Private Network (VPN) encryption and hardware advanced integration module (AIM). The symptom occurs after an IPSec SA rekeying.

  Workaround: Use the appropriate AIM-VPN-BPII-Plus or AIM-VPN/EPII-Plus or AIM-VPN/HPII-Plus AIM.

  Further Problem Description: HSP firmware version 2.3.1 was committed through CSCeg15422 to address the most common conditions that could result in PCI NULL writes that cause memory corruption. The fix for this caveat (CSCeg52468) implements HSP firmware version 2.3.2 to address additional conditions that could result in PCI NULL writes.

- CSCeg74233

  Symptoms: Some packet data protocol (PDP) contexts may not be deleted from a gateway GPRS support node (GGSN).

  Conditions: This symptom is observed when an error occurs while PDP contexts are waiting for a delete response.

  Workaround: If the PDP context exist in the Serving GPRS Support Node (SGSN), delete the PDP context from the SGSN. If the PDP context does not exist in the SGSN, there is no workaround.

- CSCeg78036

  Symptoms: The following tracebacks may be generated when VFR handles fragmented packets:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 6472EE80
  chunkmagic 0 chunk_freemagic 6484FA7C
  -Process= "IP Input", ipl= 4, pid= 60
  ```

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.3(12.11)T1 and that is configured with a virtual reassembly. The symptom may also occur on a Cisco 2651XM.

Workaround: Disable the virtual reassembly by entering the **no ip virtual-reassembly** command.

- CSCeh08689

  Symptoms: When CRTP is enabled on a PPP over Frame Relay PVC via a policy-map configuration, the service policy on the PVC does not function properly because packets are not placed in the priority queue. The output of the **show policy-map interface** command does not show a class counter.

  Conditions: This symptom is observed when you attach a policy map with CRTP on a virtual-template interface and then attach a policy map with a priority feature on the Frame relay PVC. Note that the symptom does not occur for a PPP over ATM PVC or PPP over Ethernet configuration.

  Workaround: There is no workaround.

- CSCeh35823

  Symptoms: When a router detects "invalid identity" failures while decrypting IPsec packets, a memory leak occurs for the packet memory that is associated with these failed packets.

  Conditions: This symptom is observed only when an "invalid identity" error occurs, which is an uncommon error that indicates that the originating router does not send packets according to what was originally negotiated. However, if there is another error that causes a "bad" decryption, the packet could be invalid and may also cause the symptom to occur.

  Workaround: There is no workaround.

- CSCeh40161

  Symptoms: When a branch router attempts to access the Internet via HTTP or TCP, the HTP or TCP session times out unexpectedly.

  Conditions: This symptom is observed when the router at the headquarter has a Cisco IOS Firewall and resets the HTTP or TCP connection.

  Workaround: Configure a GRE+IPSec connection between the branch router and the router at the headquarter.

  Alternate Workaround: Disable the Cisco IOS Firewall on the router at the headquarter.

- CSCeh40183

  Symptoms: A router reloads unexpectedly when the **show policy interface** EXEC command is entered.

  Conditions: This symptom is observed on a Cisco router when two users are connected to the router and simultaneously enter the **show policy interface** EXEC command.

  Workaround: Ensure that only one user at a time enters the command.

- CSCeh42852

  Symptoms: A T.37 fax fails on a Cisco 2800 series because of clocking problems with a BRI. The fax that is sent or received via the BRI may be incomplete with cut pages or a part lost. About 40 to 50 percent of the faxes fail.

  Conditions: This symptom is observed in the following topology:

  A fax is sent from a fax machine via the PSTN to a BRI on a Cisco 2800 series. The Cisco 2800 series connects via an IP interface to an SMTP mail server.

Workaround: There is no workaround. Note that a fax that is sent via FXS instead of via a BRI goes through fine.

- CSCeh60700

  Symptoms: A router that is configured for GRE+IPSec tunnel protection and VRF drops packets that are larger than the size of the MTU of the tunnel interface. The router should fragment the packets.

  Conditions: This symptom is observed on a Cisco 2600 series when the size of a (cleartext) packet is larger than 1434 bytes (which is the Ethernet MTU minus the IPSec overhead). However, the symptom is platform-independent and occurs with both software encryption and onboard hardware encryption engines.

  Workaround: On the tunnel interface that is configured for GRE+IPsec tunnel protection and VRF, configure an MTU size that is smaller than the MTU size of the physical interface of the tunnel source minus the IPSec overhead, as in the following example:

  ```
  interface tunnel0 ip mtu 1400
  ```

  (This example assumes that the physical interface of the tunnel source is an Ethernet interface with an MTU of 1500 bytes.)

- CSCeh62596

  Symptoms: A Telnet session may pause indefinitely after 13 characters or carriage returns have been accepted.

  Conditions: This symptom is observed on a Telnet session through a PVC that is configured for PPP over ATM (PPPoA).

  Workaround: If possible, use a Fast Ethernet interface for the Telnet session.

- CSCeh63526

  Symptoms: A router crashes at the insp_inspection function.

  Conditions: This symptom is observed when the inspection rule is removed and re-added to an interface while traffic passes through the interface.

  Workaround: There is no workaround.

- CSCeh65386

  Symptoms: If a crypto map has RRI enabled and is applied to more than one interface, removing the map from one interface removes all active routes that are associated with other instances of this crypto map. In particular, this situation affects dialup termination and VPN connectivity on the same physical router. When you use a virtual template, the disconnection of one virtual-access interface that is spawned from the virtual template causes all routes for all other virtual-access interfaces to be removed.

  Not all IKE and IPSec SAs on active connections are impacted, and when IPSec is rekeyed, routes are restored on the active interfaces.

  Conditions: These symptoms are observed on a Cisco router under he following conditions:

  - The same crypto map is applied to multiple interfaces.
  - RRI is configured on the crypto map.
  - VPN and dialup are configured on the same physical router.
  - There are active IPSec SAs and routes.

  Workaround: Do not remove a crypto map from an interface when there are active connections on other interfaces that use the same crypto map. First clear all SAs from the crypto map and then remove the interface.

- CSCeh72180

  Symptoms: A router may unexpectedly reload and generate the following error message:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x60FB1F70
  ```

  Conditions: This symptom is observed on a Cisco 7200 series when one interface is configured for IP Header Compression (IPHC) and when another interface has a crypto map that includes the **qos pre-classify** command. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeh76239

  Symptoms: Web Cache Communication Protocol (WCCP) may fail.

  Conditions: This symptom is observed on a router that is configured with IPSec, CBAC (that is, the **ip inspect** command is enabled), and NAT. One specific scenario in which WCCP fails is when a single interface is configured to terminate one or more IPSec tunnels and has the **ip nat outside source** command, **ip inspect out** command, and **ip wccp web-cache redirect out** command enabled.

  Workaround: When the **ip inspect out** command is enabled on the WCCP-redirected interface but the **ip inspect in** command is not configured on the client interface, configure a WCCP redirect list that excludes the address of the WCCP-redirected interface.

- CSCeh78411

  Symptoms: If a spoke cannot complete IKE phase I because of a bad certificate, the failed IKE sessions may not be deleted on an IPSec/IKE responder. Such failed sessions may accumulate, eventually causing router instability. These failed sessions can be seen in the output of the **show crypto isakmp sa | i MM** command:

  ```
  172.18.95.21    10.253.34.80   MM_KEY_EXCH        898    0 ACTIVE
  172.18.95.21    10.253.34.80   MM_KEY_EXCH        896    0 ACTIVE
  172.18.95.21    10.253.34.80   MM_KEY_EXCH        895    0 ACTIVE
  172.18.95.21    10.253.34.80   MM_KEY_EXCH        894    0 ACTIVE
  172.18.95.21    10.253.34.80   MM_KEY_EXCH        893    0 ACTIVE
  ...
  ```

  Conditions: These symptoms are observed when RSA signatures are used as the authentication method.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that is used for the IKE sessions or re-apply the crypto map to this interface.

- CSCeh91772

  Symptoms: If an existing file is extended, an ATA file system may become corrupted. When this situation occurs, the output of the **dir** command or of a **show** command does not list the files because the files are corrupted.

  Conditions: This symptom is observed when you enter any command that extends a file such as the **show interfaces ethernet | append disk0:file** command.

  Workaround: Do not enter a command that extends a file.

- CSCeh95801

  Symptoms: The domain name does not appear in the accounting records.

  Conditions: This symptom is observed when EzVPN clients use digital certifications that are terminated on a Cisco router and when RADIUS accounting is enabled.

Workaround: Use the accounting information that is available such as the Group-ID.

- CSCeh96215

  Symptoms: All platforms that support SRST may experience a crash due to memory corruption.

  Conditions: This symptom occurs when using the **translation- profile** command in call-manager-fallback configuration mode.

  Workaround: Workaround: Use the **translate** command in call- manager-fallback configuration mode.

- CSCeh96861

  Symptoms: One-way audio or no audio may occur during a call that is made through a Cisco AS5400.

  Conditions: This symptom is observed when the Cisco AS5400 functions as a terminating gateway and is connected to a Cisco 3600 series or Cisco 3800 series that functions as an originating gateway. All platforms run Cisco IOS Release 12.3(14)T. The symptom may also occur in later releases.

  Workaround: Enter the **playout-delay nominal 200** command on the voice port that is used for the call.

- CSCei01321

  Symptoms: You cannot bring up a serial interface of a channelized E1 or T1 port. The interface remains in the down/down state.

  Conditions: This symptom is observed on a Cisco 3600 series.

  Workaround: There is no workaround.

- CSCei22930

  Symptoms: When link flaps occur while a bandwidth change takes place, the QoS configurations are ignored and deleted from an ATM interface that is configured with an IMA group, and the following error messages and tracebacks are generated:

```
%SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
-Traceback= 611D46E8 6002160C 61D4EF90 602C329C 602C6574 602C6D40 61D52170
61D54F2C 61D553E8 61D55784 61D6FF84 61D550EC 61D5516C 604818FC 6047E89C
6047E9C8

%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
-Traceback= 611D46E8 600177F4 6145DCB4 6145DDFC 6146B8E8 6146E174 616AB8B0
616ABB58 6205C598 62066DE0 6205C640 61D557F0 61D6FF84 61D550EC 61D5516C
604818FC

%SYS-2-MALLOCFAIL: Memory allocation of 19 bytes failed from 0x6145DCAC,
alignment 0
Pool: Processor  Free: 139749528  Cause: Interrupt level allocation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
-Process= "<interrupt level>", ipl= 1, pid= 3
-Traceback= 611D46E8 60012958 6001822C 6145DCB4 6145DDFC 6146B8E8 6146E174
616AB8B0 616ABB58 6205C598 62066DE0 6205C640 61D557F0 61D6FF84 61D550EC
61D5516C
```

Conditions: These symptoms are observed on a multiport T1/E1 ATM network module with IMA when the ATM interface is configured with an IMA group, has the command enabled, and is configured for QoS.

Workaround: Enter the **bandwidth** command on the ATM interface that is configured with an IMA group to define the total bandwidth for all UNI interfaces of that IMA group.

Alternate Workaround: Do not configure the **atm bandwidth dynamic** command when the ATM interface is configured with an IMA group and QoS.

- CSCei23159

  Symptoms: The HSRP feature does not work on NM-16/36ESW ports configured as L3 routed ports through the **no switchport** command. HSRP works correctly on the VLAN interface and onboard L3 interfaces of the router.

  Conditions: This symptom has been observed on all routers which use NM-16/36ESW.

  Workaround: Use either of the following workarounds as necessary:

  1. Use the MAC address of the physical interface for the HSRP virtual MAC address, but this could not be applied in customer's design.

  or

  2. Enable the **standby use-bia** command under the Routed Interface as in the following example:

  interface FastEthernet1/0 no switchport ip address 10.116.216.2 255.255.255.0 standby use-bia standby 2 ip 10.116.216.1 standby 2 preempt end

- CSCei36482

  Symptoms: The output of the **show resource user iosprocess brief** command does show the resource owner (RO) and its usage by resource user (RU) but only for the first RU. Starting from the second RU, the ROs are displayed incorrectly, that is, only the buffer RO is shown. Other RO information such as CPU use are not displayed.

  Conditions: This symptom is observed on a Cisco router that has the Embedded Resource Manager (ERM) enabled.

  Workaround: Do not enter the **show resource user iosprocess brief** command. Rather, enter the **show resource owner** command as in the following example: **show resource owner cpu user iosprocess**. The output of this command shows the CPU use for the RO for all RUs in the "iosprocess" Resource User Type (RUT). Note that the symptom does not impact the functionality of the ERM or the router.

- CSCei37299

  Symptoms: A VPN hub router may reload when you enter the **clear crypto session remote** *ip-address* command.

  Conditions: This symptom is observed after a remote peer disconnects ungracefully (that is, the peer is suddenly powered-off or the LAN cable is disconnected) and immediately reconnects to the VPN hub router with a different public address.

  Workaround: Do not enter the **clear crypto session remote** *ip-address* command. Rather, enter the **clear crypto sa** command.

- CSCei41674

  Symptoms: A router may generate "SYS-2-LINKED: Bad enqueue" error messages.

  Conditions: This symptom is observed when both the following conditions are present:

  – The router generates traffic such as routing updates that are encrypted via IPSec and the traffic (packets) is process-switched after encryption.

– The router is configured with a hardware crypto accelerator.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CCSCeg43855. 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: When the error message is generated, a crash may also occur in the following configuration in which hub-n-spoke GRE tunnels are configured for IPSec and EIGRP: When the spokes have a primary hub and a backup hub (that is, a GRE tunnel to each) and when a switchover from the primary hub to the backup hub occurs multiple times, the spoke man crash. This particular situation is observed on a Cisco 1841 and Cisco 3825.

A workaround for this particular situation is to prevent multiple hub switchovers from occurring or to refrain from configuring GRE tunnels with IPSec and EIGRP.

- CSCei42842

  Symptoms: A Cisco 2851 may crash at the tsp_search_voice_port function.

  Conditions: This symptom is observed when the **no ccm-manager mgcp** command is entered very rapidly, for example, via an automated script.

  Workaround: There is no workaround.

- CSCei46509

  Symptoms: No more than 930 H.323 terminating calls can be brought up on a Cisco 5850 because socket allocation failures occur.

  Conditions: This symptom is observed on a Cisco 5850 that functions as a TGW in RPR+ mode when H.323 slow start is enabled and when H.245 tunneling is disabled. Note that the symptom does not occur when H.245 tunneling is enabled or when the Cisco 5850 functions as an OGW.

  Workaround: Configure H.245 tunneling and fast start by entering the following commands:

  ```
  Router(config)# voice service voip
  Router(conf-voi-serv)#h323
  Router(conf-serv-h323)#no h245 tunnel disable
  ```

- CSCei49745

  Symptoms: A router may crash when a certificate is revoked by entering the **crypto pki server** *cs-label* **revoke** *certificate-serial-number* command.

  Conditions: This symptom is observed on a Cisco switch or router that runs Cisco IOS Release 12.4 or Release 12.4T.

  Workaround: There is no workaround.

- CSCei50425

  Symptoms: A Cisco 7200 series or Cisco 7301 that is equipped with a VAM, VAM2 or VAM2+ accelerator may refuse a valid RSA key and generate an error message such as the following:

  ```
  % Error in generating keys: did not validate % Key pair import failed.
  ```

  Conditions: This symptom is observed under rare circumstances when a valid RSA key is composed of unusually short or long prime numbers and coefficient.

  When the VAM is deactivated during the importation of the RSA key, the router accepts the key but when the VAM, VAM2, or VAM2+ is inserted into the chassis, the router miscomputates the signature payload of the IKE/ISAKMP exchanges.

  Workaround: Create a new RSA key.

Further Problem Description: The result of the wrong operation can be seen on the other side of the connection by activating the **debug crypto engine** and **debug crypto isakmp** commands. The following messages are related to the failure:

```
crypto_engine: public key verify
crypto_engine: public key verify, got error no available resources
ISAKMP:(0:2:HW:2): signature invalid!
```

- CSCei51322

  Symptoms: A router that is configured for IPSec may reload because of a stack or program counter corruption.

  Conditions: This symptom is observed on a Cisco router that uses a certificate with a very long subject name of several hundred bytes when the distinguished name (DN) is used as an ISAKMP identity. The symptom does not occur for shorter subject names (for example, 290 characters). In most environments, a subject name of 80 characters or less is common.

  Workaround: Use certificates with a shorter subject name.

- 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.

- CSCei61814

  Symptoms: A Fast Ethernet (FE) interface on a Cisco AS5850 may reset unexpectedly.

  Conditions: This symptom is observed when you attempt to program the FE controller for multicast or broadcast traffic such as OSPF, EIGRP, RIP, or PIM.

  Workaround: There is no workaround.

- CSCei75294

  Symptoms: The 5850 chassis running in RPR + mode reloads unexpectedly with MGCP application holding memory increasing with every call and not being freed up.

  conditions: seen on as 5850 running in rpr+ with a special build of 11-T7

  workaround: None at this time

- CSCin85528

  Symptoms: A router crashes during a conference call.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured with a DSP Farm.

  Workaround: There is no workaround.

- CSCin86322

  Symptoms: An end-to-end sweep ping fails across a dLFI bundle and the bundle flaps.

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

  Workaround: There is no workaround.

- CSCin91843

  Symptoms: Auto-logon services do not automatically log on when you connect via a Service Selection Gateway (SSG).

Conditions: This symptom is observed when the user profile that is downloaded via the Access-Accept response from a RADIUS server contains a netmask (RADIUS attribute 9) that is smaller than 32 bits and when the SSG functions in PBHK mode.

Workaround: Increase the netmask bits in such a way that the bitwise and ampersand (&) operation between the netmask and the SSG PBHK source IP address results in an SSG PBHK source IP address without any alteration.

- CSCsa44556

  Symptoms: When you remove and re-enter the **zone circuit-id** command, the command may not take effect.

  Conditions: This symptom is observed on a Cisco platform that functions as a gatekeeper.

  Workaround: Reload the gatekeeper after you have made the configuration changes.

- CSCsa44852

  Symptoms: A virtual-access interface flaps continuously.

  Conditions: This symptom is observed Cisco 3745 router that functions in a PPPoA environment during normal working conditions.

  Workaround: Disable keepalives on the dialer interface on the remote router.

- CSCsa56901

  Symptoms: Cisco Fax Relay calls both to and from computer-based fax devices fail. Calls to and from traditional fax machines work fine. Calls to and from computer-based fax devices via the PSTN instead of via a Cisco Fax Relay network work fine too.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured for Cisco Fax Relay and VoIP.

  Workaround: There is no workaround.

- CSCsa59549

  Symptoms: A router that is configured for Content Based Access Control (CBAC) and Intrusion Prevention Systems (IPS) may unexpectedly reload.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T or a later release with a Cisco IOS firewall during session inspection under certain timing conditions.

  Workaround: There is no workaround.

- CSCsa61523

  Symptoms: The following error message is generated on a Cisco 7200 series that has Multilink PPP (MLP) configured on serial interfaces of a PA-MC-STM-1 port adapter:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(11)T3 only when MLP is configured on the serial interfaces. The symptom may also occur in Release 12.3 or 12.4.

  Workaround: Unconfigure MLP on the serial interfaces.

- CSCsa70040

  Symptoms: A router does not attempt to autoinstall a software configuration via a Frame Relay WAN segment when it receives a response to a DHCP request on an Ethernet LAN, even though the DHCP server does not support autoinstall via TFTP.

Conditions: This symptom is observed when a software configuration is replaced on a failed remote router or installed on a new remote router. The router is connected to an existing Ethernet LAN and a Frame Relay WAN segment. You would expected that the router autoinstalls over the Frame Relay WAN segment because it is supposed to download the configuration from a central TFTP server. However, this does not occur.

When the router has a response to its DHCP request on the Ethernet LAN, it attempts to autoinstall over DHCP. Although the DHCP server does not support autoinstall over DHCP, the router does not attempt to autoinstall over the Frame Relay WAN segment.

Workaround: Prevent the DHCP server from responding to the routerís request or ensure that someone is physically present to disconnect the Ethernet LAN link from the router to force the router to autoinstall over the Frame Relay WAN segment. When the router has autoinstalled over the Frame Relay WAN segment, the router should be reconnected to the Ethernet LAN.

- CSCsa71310

  Symptoms: An E1 controller on an MGCP trunking gateway reports Loss of Frames (LOF).

  Conditions: This symptom is observed when you configure a Cisco 3660 as an MGCP trunking gateway.

  Workaround: There is no workaround.

- CSCsa71612

  Symptoms: When you make 21 calls and place one call on hold, the callee at the PSTN side does not hear the MoH.

  Conditions: This symptom is observed on a Cisco 2621XM and Cisco 3745 that run and IP voice image of Cisco IOS Release 12.3(7)T4 and that are configured with an NM-HD-2VE, a VWIC-1MFT-T1 or VWIC-2MFT-T1, codec complexity flex, and multicast MoH.

  Workaround: Add another NM-HD-2VE and configure codec complexity medium.

- CSCsa71793

  Symptoms: A Cisco 7200 series may reload because of a bus error when you enter a **show atm** command that accesses deleted VCs structures.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(12a).

  Workaround: There is no workaround.

- CSCsa72951

  Symptoms: A DSMP-3-DSP_TIMEOUT error message may be generated when you place a fax call via a VoIP gateway.

  Conditions: This symptom is observed when the fax call is torn down and the gateway attempts to obtain call statistic information from the DSP. The DSMP state in this case is S_DSMP_COLLECTING_STATS as displayed in the error message. The timeout occurs only when MGCP PRI-backhaul mode is enabled. The symptom does not occur in standalone mode.

  The timeout itself does not impact the call for which it occurs because the timeout occurs at the end of the call while the call is being torn down and cleaned up. However, on some network modules, specifically, the 549 and 5421 DSP-based modules such as the NM-HDV and AIM network modules, when the timeout occurs, a DSP recovery mechanism is triggered and may impact other active calls on other channels on the same DSP as the one that reports the timeout. For this problem, caveat CSCsb14481 has been opened.

Although the timeout may occur on a 5510-based DSP network module such as the NM-HDV2 network module, the DSP itself does not appear to be reset so no impact to other active calls is observed.

To verify which DSP is currently in use on a gateway, enter the **show voice dsp** EXEC command.

Workaround: When MGCP PRI-backhaul is configured in a Cisco CallManager environment, you can disable Fax Relay on a gateway to prevent timeouts from occurring by entering the **no ccm-manager fax protocol cisco** global configuration command on the gateway.

Alternate Workaround: To prevent timeouts from occurring, configure the gateway to function in standalone mode.

- CSCsa73438

  Symptoms: When SSG functions in RADIUS proxy mode, SSG sends the RADIUS Framed IP Netmask Attribute value that it receives from a RADIUS server as the Framed IP Address Attribute value towards a GGSN or CSG downlink RADIUS client.

  Conditions: This symptom is observed when the RADIUS Framed IP Netmask Attribute value is less then a 32-bit mask.

  Workaround: Avoid using the RADIUS Framed IP Netmask Attribute or use a 32-bit mask value for it.

- CSCsa74930

  Symptoms: A Cisco 3825/c3845 may display the following error message and traffic is interrupted:

  ```
  %SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status =
  0x0000000000840000
  ```

  Conditions: This symptom is observed when multiple users that are connected to a downstream switch attempt to log into network resources across a WAN (traversing the router).

  Mostly Seen with Appletalk protocol over GE.

  Workaround: There is no workaround.

  Proposed Release Plan for this DDTS:

  The fix for CSCsa74930 will be integrated into:

  ```
  12.3(11)T8   CommitWindow 8/17/05-9/12/05 Likely CCO: 10/24/05
  12.3(14)T5   CommitWindow 9/20/05-10/3/05 Likely CCO: 11/14/05
  12.4(3a)     CommitWindow 7/25/05-9/01/05 Likely CCO: 10/3/05
  12.4         Commit to Hawaii before 9/10/05 so that it will also make it to
               12.4(5) CommitWindow 9/27/05 Likely CCO: 10/24/05
  12.4(2)T2    CommitWindow 9/7/05-9/19/05 Likely CCO: 10/18/05
  ```

- CSCsa85839

  Symptoms: A Cisco Aironet AIR-AP1131AG-E-K9-P access point may not function because it does not receive power.

  Conditions: This symptom is observed when an EtherSwitch NM-16ESW-PWR network module or EtherSwitch NMD-36ESW-PWR network module does not detect and supply power to the AIR-AP1131AG-E-K9-P access point.

  Workaround: Use a power injector or external power supply.

- CSCsa86555

  Symptoms: The User Adaptation Layer for a Digital Private Network Signaling System (DPNSS) path does not come up.

Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as a gateway and that run Cisco IOS Release 12.3(14)T or Release 12.4. The DPNSS path is configured on a VWIC-2MFT-E1-DI Multiflex Voice/WAN interface card that is installed in an NM-HDV2 network module.

Workaround: There is no workaround.

- CSCsa87733

  Symptoms: Only the first syslog server defined on a system receives syslog messages.

  Conditions: This symptom has been observed when more than one syslog server is defined on a router and when the **logging logging source-interface** *type instance* command is in place.

  Workaround: For those logging hosts impacted, i.e. if their message counts are not changing, if possible, enter **no logging source-interface** and then re-enter **logging 1.1.1.1** type CLI command for each configured host.

  Such as: re-enter the following 2 lines in configuration terminal mode in this case:

  ```
  logging source-interface FastEthernet1/0
  logging 192.168.104.234
  logging 192.168.104.103
  ```

  The list of hosts can be found by **show run | incl logg**.

  For those who can not do the **no logging source-interface** command. The reported problem will be there until reload with a router system image with this bug fix in reflected in it.

  Please note the underlying issue with this reported problem was due to potential port number collision after the first syslog session was added due to the way the socket library utility function was used by syslog. Therefore, this workaround may not work all the time. Only by applying the patch to this problem can definitely resolve the problem.

- CSCsa87811

  Symptoms: A memory leak occurs on an originating gateway.

  Conditions: This symptom is observed when Fast Start is enabled, when a call fails after the call proceeding has been received from a primary or alternate endpoint, and when the call falls back to the next alternate endpoint.

  Workaround: There is no workaround.

  Further Problem Description: The fast-start elements that are received in the call proceeding are freed only once for each call instead of being freed for each endpoint that is tried (assuming that the call falls back to alternate endpoints). This situation causes the memory leak.

- CSCsa89621

  Symptoms: The firewall performance of an NPE-G1 is below expectations, causing high CPU use.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(14)T1 and that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCsa94162

  Symptoms: A DHCP client router has an old static route and a new static route concurrently. The output of the **debug dhcp detail** on the DHCP client router shows that the old static route is removed but that the routing table still contains the old static route. Also, the old static route is not removed after the static configuration is deleted.

  Conditions: This symptom is observed when a DHCP server renews the DHCP address and the DHCP gateway.

Workaround: There is no workaround.

- CSCsa96494

  Symptoms: A call from an originating gateway (OGW) that is configured for SIP via an IPIPGW to a terminating gateway (TGW) that is configured for H.323 may fail when certain codecs are configured on the IPIPGW and H.323 TGW.

  Conditions: This symptom is observed under either one of the following conditions:

  – The SIP OGW is configured for g.711u, the IPIPGW for g.711u for both connections, and the H.323 TGW for g.729r8. In this configuration, the SIP OGW continues to use g.711u as the negotiated codec and discards the g.729r8 codec that is sent by the H.323 TGW via OLC.

  – The SIP OGW is configured for g.729r8, the IPIPGW for g.729r8 for both connections, and the H.323 TGW for g.711u. In this configuration, the SIP OGW continues to use g.729r8 as the negotiated codec and discards the g.711u codec that is sent by the H.323 TGW via OLC.

  Workaround: There is no workaround.

- CSCsa97663

  Symptoms: An ATM interface is unexpectedly removed from an IMA group even though the ATM interface is still in the up/up state, causing T1 links to be disconnected.

  Conditions: This symptom is observed on a Cisco 2600 series when you change the Cisco IOS software from Release 12.2(13)T8 to Release 12.3(12b).

  Workaround: Re-add the ATM interface to the IMA group by removing and reconfiguring the IMA configuration on the ATM interface.

- CSCsa98462

  Symptoms: A Cisco router may display the following error messages and then reload because of a bus error:

```
HDLC32_RX_ISR_ERR: no particles available!
HDLC32_RX_ISR_ERR: no particles available!
HDLC32_RX_ISR_ERR: no particles available!
HDLC32_RX_ISR_ERR: no particles available!

%SYS-2-BADSHARE: Bad refcount in retparticle, ptr=64689BC0, count=0
-Traceback= 0x6100C244 0x604B9F4C 0x60955894 0x60959690 0x60AFCE14 0x60AFF7E4
%ALIGN-1-FATAL: Illegal access to a low address
addr=0x0, pc=0x609560C0 , ra=0x609596BC , sp=0x6476BBF8

%ALIGN-1-FATAL: Illegal access to a low address
addr=0x0, pc=0x609560C0 , ra=0x609596BC , sp=0x6476BBF8

TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x609560C0
-Traceback= 0x609560C0 0x609596BC 0x60AFCE14 0x60AFF7E4
```

  Conditions: This symptom is observed on a Cisco router when you enter the **channel group** command to create a serial interface on an NM-HD or NM-HDV2 network module or on an onboard controller of an Integrated Services Router (ISR) such as a Cisco 2800 series or Cisco 3800 series.

  Workaround: There is no workaround.

- CSCsb01043

  Symptoms: When a Turbo ACL classification table grows beyond a certain size, a memory allocation failure may occur or the router may crash.

  If the router runs Cisco IOS Release 12.3, memory corruption may occur, causing the router to crash. If the router runs Cisco IOS Release 12.2S, an error message similar to the following may appear during a Turbo ACL compilation, the compilation will fail, and a recompilation is forced:

  ```
  %SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for TACL Block
  -Process= "TurboACL", ipl= 0, pid= 82
  ```

  These symptoms do not occur because of an out-of-memory condition.

  Conditions: This symptom is observed on a Cisco router that is configured for Turbo ACL. The Cisco 10000 series is not affected.

  Workaround: Monitor the output of the **show access-lists compiled** command and force the Turbo ACL tables to be cleared if a table is at risk of growing large enough to trigger the symptoms.

  The tables that have significant sizes are the first and third tables shown next to "L1:" and the first table shown next to "L2:". When the number after the slash for one of these tables is greater than 16384 for the "L1" tables or greater than 32768 for the "L2" table, the table is already too large and the symptom may occur any moment.

  When the number is in the range from 10924 to 16384 inclusive for the "L1" tables or the range from 21846 to 32768 inclusive for the "L2" tables, the table size will be too large on the next expansion. An expansion occurs when the number to the left of the slash reaches 90 percent of the value to the right of the slash. When the value to the left of the slash approaches 90 percent of the value to the right, enter the **no access-list compiled** command followed by the **access-list compiled** command to disable and re-enable Turbo ACL. Doing so causes the tables to be cleared and, therefore, delay the expansion. This workaround may be impractical when there is a high rate of incoming packets and when entries are added frequently to the tables.

  Alternative Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

  Note that neither of these workarounds are supported on a Cisco 7304 that is configured with an NSE-100: there is no workaround for this platform.

- CSCsb04965

  A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

  Cisco is 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-20060920-docsis.shtml.

- CSCsb06330

  Symptoms: A router may crash when you make basic IPIPGW fax calls.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T6.

  Workaround: There is no workaround.

- CSCsb06649

  Symptoms: A Cisco 3725 that is configured as an H.323 gateway does not provide three beeps for a tone-on-hold. Instead, it generates the no-circuit tone.

  Conditions: This symptom is observed on a Cisco 3725 that runs Cisco IOS Release 12.3(14)T2 and that is not configured for Music on Hold.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(11)T5.

- CSCsb06658

  A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

  Cisco is 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-20060920-docsis.shtml.

- CSCsb08192

  Symptoms: A Cisco 3800 series may not drop unicast Ethernet frames that are not destined for its MAC address.

  Conditions: This symptom is observed on a Cisco 3800 series that runs Cisco IOS Release 12.3(11)T5 or an earlier release or Release 12.3(14)T1 or an earlier release and that has subinterfaces that are configured for HSRP. The symptom may also occur on Release 12.4T.

  Workaround: Enter the **standby use-bia** command on the main interface.

- CSCsb08428

  Symptoms: A router may crash when a VPN tunnel is established.

  Conditions: This symptom is observed on a Cisco router when an interface has both IPSec and the **ip verify unicast reachable-via** command enabled and when a hardware encryption engine is used for IPSec.

  Workaround: Remove the **ip verify unicast reachable-via** command from the interface.

- CSCsb10341

  Symptoms: A Cisco 2651XM may not drop unicast Ethernet frames that are not destined for its MAC address.

  Conditions: This symptom is observed on a Cisco 3800 series that runs Cisco IOS Release 12.3(11)T5 or an earlier release or Release 12.3(14)T1 or an earlier release and that has subinterfaces that are configured for HSRP.

  Workaround: Enter the **standby use-bia** command on the main interface.

- 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

- CSCsb12405

  Symptoms: A fax call that is made over a VoIP MGCP link may fail when both the originating and terminating gateways have the **mgcp fax t38 gateway force** command enabled.

  Conditions: This symptom is observed on Cisco routers that run Cisco IOS Release 12.4 or interim Release 12.4(2.2)T.

  Workaround: There is no workaround.

- CSCsb14481

  Symptoms: Active voice and fax calls may stop unexpectedly on a gateway, that is, either the call may drop or two-way audio may stop.

  Conditions: This symptom is observed when a DSP recovery algorithm on the gateway is started in response to a DSMP-3-DSP_TIMEOUT error condition. The timeout may occur on one of the channels of the DSP, but the reset algorithm impacts other calls on other channels that are active on the same DSP.

  Network modules with 549 and 5421 DSPs such as the NM-HDV and AIM-VOICE network modules are reset when this timeout occurs, causing other active voice and fax calls on other channels of the same DSP to be reset. Network modules that use 5510 DSPs such as the NM-HDV2 network module do not seem to be reset when this timeout occurs during statistics collection.

  To verify which DSP is currently in use on a gateway, enter the **show voice dsp** EXEC command.

  Workaround: Disable the DSP recovery algorithm by entering the **test dsp recovery disable** command. However, use this command with caution because disabling the auto-recovery mechanism prevents voice and fax calls from functioning properly when a DSP enters a valid non-responding state.

  Further Problem Description: This fix for this caveat suppresses the resetting of the DSP when the timeout occurs under a statistics collection state as shown in the sample output below where the state is equal to S_DSMP_COLLECTING_STATS:

  ```
  %DSMP-3-DSP_TIMEOUT: DSP timeout on DSP 1/5:4: event 0x6, DSMP timed out,
  while waiting for statistics from the DSP. DSMP State =
  S_DSMP_COLLECTING_STATS
  ```

  The timeout may occur when an internal software error causes some invalid statistics to be polled, leading to the timeout. As an example, see caveat CSCsa72951.

- CSCsb16321

  Symptoms: The logging buffer is full with strange messages such as "readreadread."

  Conditions: This symptom is observed on a Cisco router with a 4-wire DSL WIC module that has the **logging buffered debugging** command enabled when an invalid message is accepted via the debug port TCP 1666.

  Workaround: Configure buffer logging to the informational level or lower by entering the **logging buffered informational** command.

  Access to the debug port can be blocked by deploying an interface access list that blocks access to the debug port TCP 1666 for traffic that is destined for any of the IP addresses of the router.

  For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document: http://www.cisco.com/warp/public/707/tacl.html

  For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document: http://www.cisco.com/warp/public/707/iacl.html

For information about using control plane policing to block access to the debug port, see the "Deploying Control Plane Policing White Paper:" http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

Note that the symptom does not impact other applications and services.

- CSCsb24007

  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

- CSCsb27436

  Symptoms: A Cisco platform that is configured for SSG may reload unexpectedly because of a bus error, and generate a crashinfo file that shows the following error message:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  ```

  Conditions: This symptom is observed when the **no host overlap** command is enabled and when users connect and disconnect.

  Workaround: Remove the **no host overlap** command. If this is not an option, there is no workaround.

- CSCsb28315

  Symptoms: The "tunnel protection malloc" process may cause a memory leak in the Crypto IKMP process.

  Conditions: This symptom is observed on a Cisco platform that runs a crypto image and that functions as a spoke when the interface that connects to the hub flaps and receives a new IP address after the flap.

  Workaround: There is no workaround.

- CSCsb34344

  Symptoms: A Fast Ethernet (FE) interface on a Cisco AS5400 may reset unexpectedly.

  Conditions: This symptom is observed when you attempt to program the FE controller for multicast or broadcast traffic such as OSPF, EIGRP, RIP, or PIM.

  Workaround: There is no workaround.

- CSCsb37645

  Symptoms: A router may crash during a basic H.323 call with carrier ID routing.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(3.3).

Workaround: There is no workaround.

- CSCsb40194

  Symptoms: A Cisco 7301 that is configured for SSG may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when a user with an active session logs in again. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsb46264

  Symptoms: When a dialer interface is configured as an endpoint for a IPSec+GRE tunnel, tracebacks with bad refcount may be generated.

  Conditions: This symptom is observed on a Cisco 837 when router-generated packets such as routing updates are being switched.

  Workaround: There is no workaround.

- CSCsb50143

  Symptoms: You cannot create a maximum session number for a DSPfarm profile conference.

  Conditions: This symptom is observed on a a Cisco router that runs Cisco IOS Release 12.3(11)T or Release 12.4(1a) when time slot 1 through 24 of the PRI group are configured before you attempt to create a maximum session number. The symptom occurs on an NM-HDV2 that has a PVDM2-64 installed.

  Workaround: First configure a maximum session number for the DSPfarm profile conference, then configure time slot 1 through 24 of the PRI group.

  Do not reload the gateway or enter the **shutdown** command for the DSPfarm profile after everything is properly configured because otherwise the PRI group would grasp all the DSP resources again.

Wide-Area Networking

- CSCea75722

  Symptoms: A Cisco IOS voice gateway may fail to receive a call from the public switched telephone network (PSTN) on its PRI port.

  Conditions: This symptom is observed on a Cisco 2651XM that runs Cisco IOS Release 12.2(13)T3 or Release 12.3 and that functions as a voice gateway when it does not send a Q.931 Call Proceeding message upon receiving the call.

  Workaround: There is no workaround.

- CSCee85138

  Symptoms: A SegV exception crash may occur on a Cisco router that is configured for voice calls.

  Conditions: This symptom is observed on a Cisco 2600 series that runs Cisco IOS Release 12.3(6a) or Release 12.3(9) but may not be platform-dependent.

  Workaround: There is no workaround.

- CSCeg03958

  Symptoms: A router may crash while performing an SNMP walk on VPDN-related MIB Objects. SNMP get and set operations function fine.

Conditions: This symptom is observed on a Cisco router that is configured with MLP interfaces.

Workaround: Reload the router and do not perform an SNMP walk. Instead use get operations.

- CSCeg20283

  Symptoms: E1R2 SS7 calls fail to come up when more than one call is made with the following ISDN error:

  ```
  ISDN Se1/6:15 SC **ERROR**: call_connect: call_id not found, rejecting call
  ISDN **ERROR**: Module-CCPRI Function-CCPCC_CallConnected Error-Unknown
  event received in message from L3 or Host: 4F
  ```

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(11)T.

  Workaround: There is no workaround.

- CSCeg42148

  Symptoms: Attempts to change a B-channel service state by entering the **isdn service nfas-int** *number* **b_channel** *number* **{state {0 | 1 | 2} [hard | immediate | soft]}** command appear to succeed but the service state does not change.

  Conditions: This symptom is observed when a voice application uses a B-channel. The output of the **show isdn service detail** command shows a locale of ISDN_NEAR_END_APP.

  Workaround: There is no workaround.

- CSCeg82698

  Symptoms: PPTP tunnels do not come up.

  Conditions: This symptom is observed when VPDN is configured.

  Workaround: There is no workaround.

- CSCeh06916

  Symptoms: A Cisco router crashes when PVCs are deleted while the **show pppoe session** or **show vpdn** command is entered.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for PPP over Ethernet (PPPoE) when there are two concurrent Telnet sessions. PVCs are deleted via one Telnet session while the **show pppoe session** or **show vpdn** command is entered via the other Telnet session. The symptom is platform-independent.

  Workaround: Do not delete PVCs via one session and enter the **show pppoe session** or **show vpdn** command via another session at the same time.

- CSCeh11771

  Symptoms: On a leased line (non-dialup) serial connection that is configured for PPP encapsulation, the line protocol may not come back up when the connection is reset. The PPP LCP remains in the closed state, even though the link is up physically.

  Conditions: This symptom is observed when an active PPP session is reset and when the underlying link is not simultaneously reset, that is, when PPP goes down but when the link does not go down physically. This situation would occur, for example, when a PPP session is terminated because of keepalive failures.

  Workaround: There is no workaround.

- CSCeh18018

  Symptoms: The asynchronous resources on a NAS may remain active after a VPDN setup because the LAC does not close the L2TP session on receipt of the L2TP Call Disconnect Notification (CDN) from the LNS.

Conditions: This symptom is observed on a NAS that is configured with digital modems when the L2TP session is abnormally aborted, for example, when the L2TP session is aborted before the LNS sends an LCP termination request to the dialin user.

Workaround: Manually free the asynchronous resources on the NAS by entering the **clear line** *line-number* command or ask the remote dialin user to disconnect the modem.

- CSCeh48987

  Symptoms: The CEF-Dialer feature fails to add an adjacency for a Virtual-Access1 CEF interface.

  Conditions: This symptom is observed during a test on a Cisco router that runs Cisco IOS interim Release 12.3(14.10).

  Workaround: There is no workaround.

- CSCeh62257

  Symptoms: PPP does not establish new sessions.

  Conditions: This symptom is observed on a Cisco router that is configured with full virtual-access interfaces when a PPP leak occurs.

  Workaround: Reload the router and configure virtual-access subinterfaces instead of full virtual-access interfaces.

- CSCei16649

  Symptoms: The output of the **show pppoe session** or **show vpdn session** command does not show PPPoEoA session details.

  Conditions: This symptom is observed for a point-to-point ATM interface.

  Workaround: There is no workaround.

- CSCei21549

  Symptoms: A Cisco 5850 reloads when an RLM group is unconfigured.

  Conditions: This symptom is observed when you enter the **no isdn rlm-group** *number* command and when there are more than 31 NFAS members in the same NFAS group.

  Workaround: Shut the primary interface, remove the NFAS members of the same NFAS group, and unconfigure the RLM group.

- CSCin86951

  Symptoms: An LNS router crashes on establishing a large number of PPPoA L2TP sessions.

  Conditions: This symptom is observed only when you establish sessions at a high rate. When you attempt to establish 8000 sessions, the router crashes shortly after 5000 sessions are established.

  Workaround: Establish sessions at a low rate.

- CSCsa78067

  Symptoms: A Cisco 5400HPX may crash when conditional debugging runs.

  Conditions: This symptom is observed on a Cisco 5400HPX that runs Cisco IOS Release 12.3(11)T3 when ISDN globally unique identifier (GUID) is configured.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(1a)

Cisco IOS Release 12.4(1a) is a rebuild release for Cisco IOS Release 12.4(1). The caveats in this section are resolved in Cisco IOS Release 12.4(1a) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCeg07725

  Symptoms: A router may continue to redistribute an eBGP route into EIGRP after the eBGP route is deleted or EIGRP may not redistribute an eBGP route after the eBGP route has been installed.

  Conditions: This symptom is observed on a Cisco router that redistributes eBGP routes into EIGRP when the router functions in a multihoming environment.

  The symptom occurs in a configuration with two PE routers that advertise routes via eBGP and a border router that is configured with a higher local preference than the PE routers when the eBGP route of the primary path is withdrawn and the route of the secondary path is installed.

  Workaround: If a route is still redistributed into EIGRP after the eBGP route is deleted, clear the BGP peer from which the eBGP route used to be learned so EIGRP stops advertising the route.

  If a route is not redistributed into EIGRP after an eBGP route is installed, clear the route so EIGRP starts advertising it. Another workaround is to enter the **bgp redistribute-internal** command to cause EIGRP to redistribute iBGP routes and to prevent EIGRP from failing to redistribute an updated BGP route.

- CSCeg58039

  Symptoms: Border Gateway Protocol (BGP) could crash.

  Conditions: This symptom occurs when the max-paths value is modified.

  Workaround: There is no workaround.

- CSCeh33504

  Symptoms: A router terminates 102,000 VPNv4 routes but route reflectors (RRs) report only a a subset of the total.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs Cisco IOS Release 12.3(11)T4 when 204 routes are configured per VRF over 496 VPNs (one VPN has about 1000 routes). However, Cisco MGX RPM-PRs that function as RRs show that only 76245 routes are terminated on the Cisco MGX RPM-XF. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCeh47763

  Symptoms: A Cisco router may erroneously send ACK packets in response to RST packets for non-local TCP sessions. This can cause high CPU utilization on the router.

  Conditions: This symptom occurs when using Port Address Translation (PAT).

  Workaround: Use the **clear ip nat translation *** command.

- CSCsa54937

  Symptoms: An LNS with a VRF configuration does not send an echo reply when it receives a ping to loopback interface 0.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-300, a Cisco 7200 series that is configured with an NPE-400, and a Cisco 7400 series.

Workaround: Wait about 20 minutes to enable the LNS to send an echo reply or enter the **clear arp-cache** command.

Miscellaneous

- CSCee17241

  Symptoms: When the redundancy mode is changed from classic-split to RPR-plus through the command line interface (CLI), the peer Route Switch Controller (RSC) goes to the initial configuration setup dialogue.

  Conditions: This symptom has been observed on a Cisco AS5850 universal gateway.

  Workaround: Load the configurations with RPR-plus configured onto the startup configurations of both RSCs. The symptom will not be seen.

- CSCee42932

  Symptoms: Resuming a call that was placed on hold fails on a Cisco CallManager.

  Conditions: This symptom is observed when a Cisco CallManager that runs version 4.0 and that is not configured for Message Transport Protocol (MTP) is connected via an IPIPGW to another Cisco CallManager that runs version 4.0 and that is not configured for MTP.

  The symptom occurs on the second Cisco CallManager because the IPIPGW sends an incorrect ICT version for the first Cisco CallManager to the second Cisco CallManager and because the IPIPGW drops the non-standard fields in the callproc, alert, and connect messages from the second Cisco CallManager to the first Cisco CallManager.

  Workaround: Configure MTP.

- CSCee78300

  Symptoms: A bus error crash (that is, an illegal access to a low address) may occur in the RADIUS process.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1 and that runs Cisco IOS Release 12.3(9).

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(3).

- CSCef72756

  Symptoms: A Cisco IP phone may not have access to network resources because it cannot perform TTP-, FTP-, or Telnet-based authentication.

  Conditions: This symptom is observed on a Cisco IP phone that is connected behind a Cisco router on a interface that is configured for Authentication Proxy.

  Workaround: Add the Cisco IP phone source IP address as a “deny entry” in the Authentication Proxy Intercept ACL so that IP phone is bypassed for authentication, and ensure that the interface ACL has a permit statement for the IP phone.

- CSCeg53478

  Symptoms: A Cisco 831 may display the following message on the console:

  ```
  pktFlowLink() logic error, pMatch and pEmptySlot
  ```

  Conditions: This symptom is observed very rarely after the router has been up for a long time. The functionalities of the router are not affected.

  Workaround: There is no workaround.

- CSCeg70465

  Symptoms: There is no QoS classification at a main interface when packets are switched from a GRE tunnel that also has a QoS policy enabled.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3T or Release 12.4 when a QoS policy is enabled on both the GRE tunnel and the main interface in the output direction.

  Workaround: Move the complete QoS configuration to the QoS policy on the main interface (that is, use an hierarchical policy).

- 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.

- CSCeg89017

  Symptoms: MGCP calls fail with a fast busy signal. When you enter the **debug mgcp packet** command, the output indicates that the 400 Voice Call Setup failed.

  Conditions: This symptom is observed when MGCP PRI backhaul is configured on a Cisco 2800 series that is configured with PVDM2 DSPs. Calls fail only after the router is reloaded. The symptom may also occur on a Cisco 3800 series that functions in the same configuration.

  Workaround: Enter the following sequence of commands:

  1. Enter the **ccm-manager config server** *ip-address* command followed by the **ccm-manager config** command.
  2. Enter the **shutdown** command on the voice port or on the T1 controller.
  3. Enter the **no mgcp** command followed by the **mgcp** command.
  4. Enter the **no ccm-manager config** command followed by the **ccm-manager config** command, assuming that you have the TFTP server defined.
  5. After you reload the router, enter the **write erase** command, add the configuration, and save the configuration.

- CSCeg89043

  Symptoms: A Cisco gateway may reload unexpectedly because of a SegV exception at address PC 0x80FF6340.

  Conditions: This symptom is observed when the gateway is configured for VoIP and fallback to an SNMP trap.

  Workaround: There is no workaround.

- CSCeh05968

  Symptoms: Distributed Sessions Manager (DSM) is flooded with DSP stats messages.

  Conditions: This symptom is observed when the event pool is out of events.

  Workaround: There is no workaround.

- CSCeh14272

  Symptoms: Prioritized encrypted traffic is dropped.

  Conditions: This symptom is observed when the Low Latency Queuing (LLQ) for IPSec Encryption Engines feature is enabled.

  Workaround: Disable QOS preclassification on the crypto map.

- CSCeh14446

  Symptoms: The maintenance mode on a Cisco AS5850 that is configured for RPR+ may not function.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(11)T.

  Workaround: There is no workaround.

- CSCeh17995

  Symptoms: When you enter the following commands on the Fast Ethernet port of an NM-16ESW network module, the router may crash:

  ```
  ip dhcp client hostname
  no switchport mode
  switchport mode
  ```

  Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series in which an NM-16ESW network module is installed.

  Workaround: Do not enter IP commands in switchport mode.

- CSCeh32576

  Symptoms: Configuring an AUX port through a non-slotted notation such as “interface async 1”may not be possible on a Cisco 1841 and a Cisco 2801.

  Conditions: This symptom is observed on a Cisco 1841 and Cisco 2801 that run Cisco IOS interim Release 12.3(11.9)T or a later release.

  Workaround: Configure the AUX port through the slotted notation such as “interface async 0/0/0”.

- CSCeh35324

  Symptoms: Weighted Random Early Detection (WRED) does not match packets based on any marking done.

  Conditions: This symptom has been observed when qos pre-classification (the **qos pre-classify** command) is turned on.

  Workaround: Remove the **qos pre-classify** command.

- CSCeh35411

  Symptoms: A 4-port OC-12 POS Engine 2 line card may crash repeatedly when the Cisco 12000 series in which the line card is installed comes up after a software-forced crash has occurred on the router.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S, that is configured with two RPS, and that is configured for SSO. The symptom is more likely to occur when the **ipv6 unicast-routing** command is enabled.

  Workaround: To diminish the chance that the symptom occurs, disable the **ipv6 unicast-routing** command.

- CSCeh35457

  Symptoms: Policy-maps can be removed from the ATM PVC Range configuration without checking for an exact match of the policy-map name.

  Conditions: If a **no policy-map out** command is executed on a subinterface while the subinterface is in Admin Shutdown state, any policy-map could be deleted regardless of whether the name of the policy- map name to be removed matches with the configured policy-map or not. This problem only occurs in the PVC Range configuration on ATM subinterfaces.

  Workaround: There is no workaround.

- CSCeh42620

  Symptoms: Authentication, Authorization, and Accounting (AAA) for IKE fails with the following message when trying to begin session accounting:

  ```
  ISAKMP AAA: Unable to allocate AAA User ID: no peer
  ```

  Conditions: This error occurs when IKE accounting is configured in a site-to-site IPSec VPN. It will not occur when IKE accounting is configured in conjunction with mode configuration, XAUTH or EZVPN.

  Workaround: There is no workaround.

- CSCeh49462

  Symptoms: Tracebacks are found on a Cisco AS5850 with bulk analog and digital calls. This is not service impacting. Calls are landing on the Cisco AS5850.

  Conditions: This symptom is observed when running stress on a Cisco AS5850 with ERSCs.

  Workaround: There is no workaround.

- CSCeh61337

  Symptoms: You can change the *milliseconds* argument of the **ip icmp rate-limit unreachable** *milliseconds* command or the **ip icmp rate-limit unreachable DF** *milliseconds* command, but the new time limit does not take effect even though the configuration reflects the new time limit.

  Conditions: This symptom is observed on a Cisco MGX RPM-XF that runs a Cisco IOS Release 12.3(11)T5 or an earlier 12.3T release.

  Workaround: There is no workaround.

- CSCeh62694

  Symptoms: Cannot logout/do not disturb (DND) all agents within an ephone hunt group before starting the BACD script.

  Conditions: This symptom is observed on a Cisco gateway that has an ephone hunt group configured.

  Workaround: There is no workaround.

- CSCin86923

  Symptoms: A PVC is unexpectedly removed from an IMA interface that is reconfigured.

  Conditions: This symptom is observed on a Cisco router when an IMA interface is down and when the IMA interface is reconfigured with a service policy or when you enter the **oam-pvc manage** command.

  Workaround: Re-add the PVC to the IMA interface.

- CSCsa57147

  Symptoms: A disconnect event is not thrown or caught on a Cisco AS5400.

Conditions: This symptom is observed when the platform functions under a heavy load with a large number of calls that are disconnected from the gateway during VXML page execution. The disconnect event may not be thrown or get caught by the catch blocks of the root document.

Workaround: There is no workaround.

- CSCsa59667

  Symptoms: An AIM that is installed in a Cisco 2851 or Cisco 3845 may time out when it receives non-multiples of a 64-bits public key from a third-party vendor router. This situation causes the router to crash rather than verifying the key.

  The Cisco 2851 crashes because of a memory corruption. The Cisco 3845 crashes because of an "ALIGN-1-FATAL" bus error.

  Conditions: This symptom is observed on a Cisco 2851 and Cisco 3845 that run Cisco IOS Release 12.3(11)T3.

  Workaround: Ensure that the AIM receives multiples of the 64-bits public key.

  Alternate Workaround: Disable the AIM hardware encryption by entering the **no crypto engine aim 0** command. Doing so causes onboard encryption to occur.

- CSCsa62681

  Symptoms: SIP messages from Cisco IOS gateways fail to reach the remote endpoint. This is seen for UDP transport only.

  Conditions: This symptom happens when interworking with a third party SIP device, which sends responses to SIP Requests to the source port of the request packet instead of sending them to the header port (5060). This is in violation of the RFC3261 rules for UDP (unreliable transports).

  Workaround: There is no workaround.

- CSCsa63019

  Symptoms: A security gateway may crash when ISAKMP accounting is enabled at aggressive time intervals such as 1-minute updates.

  Conditions: This symptom is observed when ISAKMP accounting is enabled at very frequent update intervals together with ISAKMP NAT-T.

  Workaround: Use ISAKMP accounting timers with a longer duration.

- CSCsa66255

  Symptoms: IP data traffic does not pass via MLP.

  Conditions: This symptom is observed on a Cisco 3825 that runs the c3825-advsecurityk9-mz image of Cisco IOS Release 12.3(11)T3 when STAC compression on an AIM-COMPR4 fails.

  Workaround: There is no workaround.

- CSCsa68004

  Symptoms: Service Selection Gateway (SSG) does not update tariff switch information to the users when the user logs in exactly at tariff switching time.

  Conditions: This symptom is observed for postpaid users only.

  Workaround: There is no workaround.

- CSCsa68228

  Symptoms: A Cisco router may crash when using the **dialplan- pattern** command.

  Conditions: This symptom is observed when a router is configured with a high number of ephone-dns and with the application of the **dialplan- pattern** command.

Workaround: There is no workaround.

- CSCsa68768

  Symptoms: After fallback occurs from CCM to secure a Survivable Remote Site Telephony (SRST) gateway (GW), during full-consult transfer from a secure to nonsecure IP phone and then back to a secure IP phone, which are all in single line mode, one-way voice is heard. There is a loud noise on the other side.

  Conditions: This symptom happens only when the transfer-system is full- consult, and there is a nonsecure to secure call transfer.

  Workaround: Use IP phone with dual line.

- CSCsa68978

  Symptoms: Memory allocation (malloc) failures may occur on a Cisco router that functions as a gatekeeper and that runs an H.323 stack.

  Conditions: This symptom is observed on the gatekeeper when gateways attempt to register a list of terminal aliases that consists of user names and H.323 IDs with the gatekeeper. The gatekeeper attempts to authenticate each terminal alias by allocating memory and sending an authentication request to the AAA server for each entry. Because the gatekeeper does not free the allocated memory when it receives a response from the AAA server, a memory allocation failure occurs eventually.

  Workaround: There is no workaround.

- CSCsa69690

  Symptoms: The night service toggle code does not work properly with shared Directory Numbers (DNs).

  Conditions: This symptom is observed when the DN is shared on multiple phones.

  Workaround: There is no workaround.

- CSCsa72085

  Symptoms: Two Cisco 7970 IP phones that function in secure SRST single line mode lose their secure mode.

  Conditions: This symptom is observed when the following sequence of events occurs:

  1. IP phone A calls IP phone B.
  2. IP phone B answers, causing IP phone A and IP phone B to be connected and secure.
  3. The Confirm button is pressed, causing “No line available” to be displayed because the mode is single line, not dual line. At this point, IP phone A and IP phone B are still connected and secure.
  4. Hold and resume is selected, causing the IP phones to lose their secure mode. The call is no longer secure.

  Workaround: There is no workaround.

- CSCsa73120

  Symptoms: A Cisco IPSec router may restart because of a bus error.

  Conditions: This symptom is observed when you remove a crypto map entry that includes the **dynamic** keyword in its definition, as in the following example:

  ```
  router#show running
  ...
   crypto map map-name 5 ipsec-isakmp dynamic dyn-map
  ```

```
...
 router(config)#no crypto map map-name 5
```

Workaround: Before you delete the crypto map entry that includes the **dynamic** keyword in its definition, manually configure all dynamic crypto maps to point to a nonexistent ACL, as in the following example:

```
router#show running
...
 crypto dynamic-map dyn-map 5
...
 router(config)#crypto dynamic-map dyn-map 5
 router(config-crypto-map)#match address no-such-acl
```

- CSCsa73842

  Symptoms: An IP phone line is not released for some calls between Cisco CallManagers.

  Conditions: This symptom is observed when calls between the Cisco CallManagers are made via a Cisco Multiservice IP-to-IP Gateway (IPIPGW) that is configured for H.323.

  Workaround: There is no workaround.

- CSCsa78779

  Symptoms: A memory leak may occur in the processor memory pool of a router that runs encrypted traffic with an SA-VAM2.

  Conditions: This symptom is observed when the SA-VAM2 encrypts traffic and when underlying "no buffer" conditions exist in the I/O particle pools for the encrypted packets.

  Workaround: There is no workaround.

- CSCsa86918

  Symptoms: A clicking sound is heard after each .wav audio file is played from a VoiceXML (VXML) document.

  Conditions: This symptom occurs in Cisco IOS Release 12.3(14)T on a Cisco AS5400. The problem only occurs when there are multiple .wav files in a single VXML document that are concatenated together to play to the caller. A VXML document containing a single .wav file does not experience the problem.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCeg22171

  Symptoms: Calls fail to connect when they are switched from the primary D channel to the backup D channel.

  Conditions: This symptom is observed when you either unplug the cable or shut down the controller of the primary D channel.

  Workaround: There is no workaround.

- CSCeg22533

  Symptoms: A signal-only call fails when an INVALID message is generated because a B-channel IDB is not found.

Conditions: This symptom is observed when ISDN PRI QSIG Voice Signaling is configured.

Workaround: There is no workaround.

- CSCeg55098

  Symptoms: When an ISDN switch deactivates layer 2, a router immediately activates layer 2. The output of the **debug isdn q921** command shows that the router activates layer 2 within 6 milliseconds:

  ```
  ISDN BR0 Q921: User RX <- DISCp sapi=0 tei=65
  ....
  BR0 Q921: User TX -> UAf sapi=0 tei=65
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T2 and that is configured with a BRI. Note that the symptom does not occur in Release 12.3(11)T.

  Workaround: There is no workaround. However, to prevent the consecutive line up/down messages from being generated, enter the following interface configuration commands:

  interface *bri number*
  no logging event link-status

- CSCeg88174

  Symptoms: Drops occur in a class in which the throughput does not oversubscribe the allocated bandwidth for the class.

  Conditions: This symptom is observed when multilink Frame Relay is configured along with generic traffic shaping or Frame Relay traffic shaping and when several class maps are configured.

  When one class map starts dropping packets because the throughput is greater than the allocated bandwidth (which is normal behavior), drops may also occur in another class map even though this class map is not oversubscribed. The root cause of this symptom is that the bundle is oversubscribed and tx rings are building up, causing excessive misordering that the receiver cannot handle.

  Workaround: Configure a fancy queue on the bundle interface through which the traffic is sent.

- CSCeh33185

  Symptoms: A POS interface on a VIP4-80 that is configured for PPP goes down and remains down.

  Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0S only when PPP receives an LCP PROTOCOL REJECT message for PAP or CHAP. The symptom may also occur in other releases.

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

- CSCeh59311

  Symptoms: None of the digits in INFO messages are passed to an ISDN switch.

  Conditions: This symptom is observed on a Cisco 1760 that runs Cisco IOS Release 12.3(11) or Release 12.3(11)T4 when overlap is configured and when the setup acknowledgement arrives late from the terminating switch after some of the INFO messages have already been received from the OGW. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsa81268

  Symptoms: A Cisco AS5850 may reload with a software forced crash.

  Conditions: This symptom occurs when configuring the **isdn ie oli** interface command.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(1)

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

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.

- CSCee83917

  Symptoms: The RP of a Cisco router may crash when entering the **write memory** legacy command.

  Conditions: This symptom is observed on a Cisco router that has the **snmp mib community-map** command enabled with a very long community string and an engineID. The symptom may also occur when the long community string is removed from the configuration. The symptom does not occur when entering the **copy running-config startup-config** EXEC command.

  Workaround: A community string that is shorter than 40 characters will not cause the symptom to occur.

- CSCef84254

  Symptoms: When the ATM Software Segmentation and Reassembly (SAR) feature is enabled, OAM drops may occur, which may cause PVCs to go down.

  Conditions: This symptom is observed on a Cisco 2600 series and Cisco MC3810 that have ATM PVCs that are configured for any type of ATM QoS (VBR-nrt, UBR, UBRr+, and so on) and that have VCs that function at less than the line rate.

  Workaround: Configure a VC (with any QoS type) to function at the line rate.

  Possible Alternate Workaround: Remove the OAM configuration.

- CSCeg41734

  Symptoms: The console of a router may stop responding and the router may stop forwarding traffic.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(6b) and that is configured with an NPE-G1 when the native Gigabit Ethernet interfaces of the NPE-G1 are used. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg62206

  Symptoms: High CPU utilization may occur during the TPLUS process on a platform.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(6c) and that is configured for TACACS.

  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.

- CSCeg71686

  Symptoms: With the QoS Portchannel running traffic, the route processor (RP) crashes when resetting a PWAN2+ linecard through the **hw module 4 reset** command. This is a PWAN2+ card at slot 4.

  Conditions: The symptom has been observed while executing the **hw module 4 reset** command with QoS QinQ/Portchannel configurations.

  Workaround: Disable the **cdp** command in global configuration mode by entering the **no cdp run** command.

- CSCeg77984

  Symptoms: Traffic does not go properly through an IPSec tunnel: many packets are dropped.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(12.12)T1 or interim Release 12.3(12.12)T2 when software encryption is configured.

  Workaround: Use hardware encryption.

- CSCeh16064

  Symptoms: When you enter the **snmp-server host** *host-address* **public frame-relay isdn envmon cpu voice snmp** global configuration command, the command is saved to the configuration as **snmp-server host** *host-address* **public frame-relay isdn envmoncpu voice snmp**. (Note that "envmon" and "cpu" are saved as "envmoncpu".) When you reload the platform, the command is removed from the configuration because its syntax is improper.

  Conditions: This symptom is observed in Cisco IOS Release 12.3(11)T3 and is platform-independent.

  Workaround: Enter the **snmp-server host** *host-address* **public** command to enable all the traps.

- CSCeh47604

  Symptoms: An OER border component does not sent passive updates for OER prefixes, preventing the prefixes from being controlled. The prefixes cycle from the default state to the hold-down state back to the default state.

  Conditions: This symptom is observed when NetFlow is configured and when the mode monitor is configured to be "passive" or "both".

  Workaround: Configure the mode monitor to be "active". The functionality of the mode monitor is limited to the "active" mode only.

- CSCin80513

  Symptoms: An SSG platform crashes because of a memory corruption.

  Conditions: This symptom is observed when SSG processes prepaid RADIUS proxy users and is most likely to occur when a tunnel authentication failure for a prepaid RADIUS proxy user occurs.

  Workaround: There is no workaround.

- CSCin88970

  Symptoms: Using snmpwalk on the ciscoEntityFRUControlMIB leads to a system crash.

  Conditions: If the platform doesn't support cefcFRUPowerStatusTable and cefcFRUPowerSupplyGroupTable in CISCO-ENITY-FRU-CONTROL-MIB, the system may pause indefinitely. Most of the platforms don't support this MIB.

  Workaround: Either exclude ciscoEntityFRUControlMIB from the view or exclude cefcFRUPowerStatusTable and cefcFRUPowerSupplyGroupTable from the view.

- CSCsa53912

  Symptoms: You cannot log on when a TACACS+ server is used for authentication. You get a message that authentication fails and you are asked again to enter your user name.

  Conditions: This symptom is observed when you make a Telnet connection to a router that is configured for TACACS+ after you have entered you user name and your TACACS password.

  Workaround: Configure the TACACS+ single connection option by entering the **tacacs-server host** *host-name* **single-connection** command.

- CSCsa64398

  Symptoms: A router crashes because of a SegV exception when you enter the **show running-config** command via a Telnet session into the router.

  Conditions: This symptom is observed on a Cisco 828 that runs Cisco IOS interim Release 12.3(12.12)T3 and that is configured for AAA via a TACACS+ server.

  Workaround: Enter the **show running-config** command on the console of the router.

EXEC and Configuration Parser

- CSCeg60079

  Symptoms: You cannot configure the **atm pppatm passive** command on both an ATM main interfaces or ATM subinterfaces.

  Conditions: This symptom is observed on a Cisco 7200 series that runs the c7200-is-mz image of Cisco IOS interim Release 12.3(12.12)T1. The symptom also affects the Cisco 7301.

  Workaround: There is no workaround.

- CSCeg87083

  Symptoms: When entering via SSH, view-based users are not authorized to access their view but are authorized according to their corresponding privilege level.

  Conditions: This symptom is observed on a Cisco platform that is configured for Role Based Access Control (RBAC).

  Workaround: There is no workaround.

IBM Connectivity

- CSCeg78046

  Symptoms: A router that is configured for BSTUN and BIP may generate an "%ALIGN-3-SPURIOUS" memory access error message.

  Conditions: This symptom is observed when you change the BSTUN BIP configuration on an interface that is processing traffic.

  Workaround: Shut down the interface that is configured for BSTUN and BIP before you make any configuration changes.

- 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

- CSCea29435

  Symptoms: A VC that is configured on an ATM PA-A3 port adapter may stop receiving traffic.

  Conditions: This symptom is observed on a Cisco 7x00 router that is configured with an ATM PA-A3 port adapter when the default MTU is changed to a higher value.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface on which the VC is configured.

- CSCef23253

  Symptoms: When you activate a serial interface on a PA-MC-8TE1+ port adapter that is installed in a VIP, dCEF may be disabled on the slot in which the PA is installed (in this example, in slot 3) and the following error message is generated:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 3: IPC Failure: timeout
  ```

  The output of the **show controller vip 3 logging** command may time out, indicating problems with IPC.

  The failure may cause additional error messages or may cause the VIP to reset, affecting all port adapters that are installed in the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series with a faulty PA-MC-8TE1+ port adapter that is installed in a VIP.

  Workaround: There is no workaround. This fix for this caveat eases the detection of a faulty port adapter (see below).

Further Problem Description: The fix for this caveat will detect and shut down a faulty port adapter so that the VIP and the other port adapters in the VIP are not affected. The error message that is added by the fix is the following:

```
%VIP2 R5K-1-MSG: slot3 PA BAD - disabling the PA in bay 1
```

This message indicates that the PA-MC-8TE1+ in bay 1 is faulty and must be replaced.

- CSCef44950

  Symptoms: ISDN is not properly established.

  Conditions: This symptom is observed on a Cisco 7500 series that has distributed switching enabled via the **ip cef distributed** command.

  Workaround: Disable distributed switching.

- 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.

- CSCeh17935

  Symptoms: When you perform an Online Insertion and Removal (OIR) of an ATM port adapter, tracebacks are generated.

  Conditions: This symptom is observed on a Cisco 7200 series when the ATM port adapter is up and has a VC configured, when traffic passes through the ATM interface of the port adapter during the OIR, and when the ATM interface of the port adapter is oversubscribed.

  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.

- CSCin86673

  Symptoms: A VC may become stuck and stop transmitting traffic.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-A3 or PA-A6 port adapter when there is a high traffic load and when the QoS class of the VC is changed.

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

IP Routing Protocols

- CSCef11304

  Symptoms: When performing a snmpwalk on OSPF-MIB that supports the ospfExtLsdbTable, a router can crash. In other instances alignment errors are observed when you enter the **show alignment** command.

  Conditions: These symptoms are observed on a Cisco platform that runs Open Shortest Path First (OSPF) and supports the ospfExtLsdbTable in OSPF-MIB.

  Workaround: There is no workaround.

- CSCef33035

  Symptoms: A router may crash and reload and generate the following error message:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x609EE524
  ```

  Conditions: This symptom is observed on a router that runs OSPF and that is configured with incremental SPF (ISPF).

  Workaround: Disable ISPF by entering the **no ispf** router configuration command.

- CSCef60452

  Symptoms: A router may stop receiving multicast traffic.

  Conditions: This symptom is observed rarely during convergence when a router receives a Join message on an RPF interface and when a downstream router converges faster than the first router that receives the Join message.

  In this situation, the router does not populate the RPF interface into the OIL (that is, the OIL remains null) because the old SP-tree has already been pruned by the downstream router. When the RPF interface of the router changes to the new path later, it does not trigger a Join message toward the multicast source until the router receives a next periodic Join message from the downstream router and populates the OIL. As a result, multicast traffic stops temporarily but no longer than the periodic Join message interval.

  Workaround: There is no workaround.

- 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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef85199

  Symptom: The router can crash when there is continuous flow of traffic and entire mroute table is cleared via **clear ip mroute *** command or unconfiguring multicast.

  Conditions: This symptom is observed during a test on a Cisco router with the Network Service Engine 100 (NSE-100) when there is continuous flow of traffic and entire mroute table is cleared via **clear ip mroute *** command or unconfiguring multicast. The crash was only seen on a Cisco router with the Network Service Engine 100 (NSE-100).

  Workaround: There is no workaround.

- 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.

- CSCef95026

  Symptoms: When interfaces flap, a Cisco router may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when OSPF accesses a freed LSDB entry.

  Workaround: There is no workaround.

- CSCeg19442

  Symptoms: A router that is configured with the OSPF routing protocol may reload.

  Conditions: This symptom is observed when the OSPF process is simultaneously deconfigured via one session and configured via another session.

  Workaround: There is no workaround. Cisco strongly discourages you to configure a router via two different but simultaneous sessions.

- CSCeg30291

  Symptoms: BGP fails to send an update or withdraw message to some peers when these peers have failed to converge properly after an earlier attempt.

  Conditions: This symptom is observed on a Cisco router when you enter the **clear ip bgp** *neighbor-address* **soft out** command while BGP is in the middle of converging. The symptom does not occur when network traffic load is low and BGP has converged.

  Workaround: To clear the error condition, enter the **clear ip bgp** *neighbor-address* **soft out** command again. Alternately, enter the **clear ip bgp** *neighbor-address* command (that is, without the **soft out** keyword).

- CSCeg35811

  Symptoms: A platform (that is, a switch or a router) may crash when you enter the **ip routing** command followed by the **configure memory** command and the **no ip routing** command multiple times. Multiple tracebacks may also be generated.

  Conditions: The symptom is observed on a Cisco platform that functions as the master in a stacked environment and that is configured for OSPF. The symptom is more likely to occur when the platform functions under a heavy traffic load.

  Workaround: Do not enter the **ip routing** command followed by the **configure memory** command and the **no ip routing** command multiple times.

- CSCeg52659

  Symptoms: A Cisco 7200 series may not withdraw a BGP route from an iBGP peer.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) when the **clear ip bgp** *neighbor-address* **soft out** command is entered for one of the members of the peer group of which the Cisco 7200 series is a member and when some changes to the outbound policy are made to the same member of the peer group. This situation causes some prefixes to remain struck in the other members of the peer group.

  The symptom is a very old behavior of the BGP peer group functionality: when one member of a peer group is cleared via either a hard reset or a soft reset and a policy change causes some of the prefixes to be withdrawn, inconsistencies may occur in the routes on the other members of the peer group.

  Workaround: For peer groups and neighbors that are members of a peer group, do not enter the BGP neighbor-specific **clear ip bgp** *neighbor-address* **soft out** command or the **clear ip bgp** *neighbor-address* command. Rather, enter the peer group-specific **clear ip bgp** *peer-group-name* **soft out** command or the **clear ip bgp** *peer-group-name* command.

- CSCeg52889

  Symptoms: TE tunnels do not come up.

  Conditions: This symptom is observed when a new loopback interface is created with an IP address on an MPLE TE head router that is configured with MPLS TE tunnels and when you reload the router. The symptom occurs because of a change in router ID.

  Workaround: Shut down the newly created loopback interface, save the configuration, and reload the router.

- CSCeg70726

  Symptoms: A router may crash when you enable MVPN by entering the **mdt default** *group-address* command under a VRF.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  Workaround: There is no workaround.

- CSCeg72254

  Symptoms: A router reloads when you clear NAT entries from the NAT table.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(7)T7 only when Stateful Network Address Translation (SNAT) is configured on the router.

  Workaround: There is no workaround.

- CSCeg74205

  Symptoms: In a simple network that consists of two routers, SPF calculations occur every minute although no topology changes occur.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS release later than Release 12.3(6b) or Release 12.3(7)T4 and that functions as an ABR router when there are static routes in the network.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(6b) and Release 12.3(7)T4: SPF calculations do not occur every minute.

- CSCeg81061

  Symptoms: An inside client cannot make an FTP connection to an inside FTP server by using the global IP address of the server.

  Conditions: This symptom is observed when a NAT virtual interface is configured on a Cisco router that is the default gateway for the FTP client and FTP server that are both located behind the router.

  Workaround: Make a connection by using the local IP address of the FTP server.

- CSCeg89246

  Symptoms: When overlapping global addresses are configured and when there is a flow entry, the wrong entry may be matched.

  Conditions: This symptom is observed on a Cisco platform that is configured for NAT when all five tuples, except the VRF ID, are the same for two flows.

  Workaround: There is no workaround.

- CSCeh07809

  Symptoms: When BGP nexthop information for a prefix changes because of topology changes, BGP properly updates its path information and IP routing table entry but CEF may not update the corresponding CEF entry, causing a stale entry. This inconsistency between BGP and CEF may cause a connectivity problem.

  Conditions: This symptom is observed when the nexthop information changes to an existing prefix entry in the BGP routing table. Typically, this occurs when the interface through which the prefix is learned goes down.

  Workaround: Flush out the stale CEF entry by entering the **clear ip bgp** command or withdraw and readvertise the prefix by the source router, which enables the affected router to refresh the CEF entry.

- CSCeh14015

  Symptoms: Connected routes cannot be redistributed from one protocol to another.

  Conditions: This symptom is observed on EIGRP routes when you enter the **shutdown** command followed by the **no shutdown** command. The symptom may also affect other routing protocols.

  Workaround: There is no workaround.

- CSCeh24147

  Symptoms: The implementation of IPv6 scope support in the Bootstrap Router (BSR) mechanism may cause interoperability problems.

  Conditions: This symptom occurs because the specification of IPv6 scope support in the BSR mechanism has changed in the latest IETF draft:
  http://www.ietf.org/internet-drafts/draft-ietf-pim-sm-bsr-05.txt

  Workaround: Do not use IPv6 scope support in the BSR mechanism.

- CSCin87277

  Symptoms: CPUHOG messages are generated when you bring up OSPF adjacencies on hundreds of subinterfaces.

Conditions: This symptom is observed when LSAs are configured to be refreshed every 30 minutes.

Workaround: There is no workaround.

- CSCsa55555

  Symptoms: A router may reload because of a bus error when the NAT MIB is polled via SNMP.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T2.

  Workaround: There is no workaround.

- 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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa67785

  Symptoms: Packets may be dropped on the interface when NAT/IPSEC/IPS is configured on the same interface.

  Conditions: If IPSec/NAT and CBAC or IPS/IDS is configured on the same interface and the packet gets punted by any of the features, then the packet may be dropped.

  Workaround: Remove from the configuration the feature which punts the packet to process path.

- CSCuk54787

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

ISO CLNS

- CSCeh00090

  Symptoms: Routes may be unexpectedly removed from the routing table.

  Conditions: This symptom is observed when IS-IS is used to advertise IP prefixes and when you enter a **distance** command that changes the overall configuration but keeps a subset of the prefixes at the same distance as in the previous configuration. The routes for which the distance does not change may be removed from the routing table.

  The following two examples show configurations in which the symptom occurs. When the distance configuration for IS-IS is **115 ip** and you enter one of the following command sequences, the symptom occurs:

  ```
  router isis distance 255 ip distance 115 ip
  ```

  or

  ```
  router isis distance 115 0.0.0.0 255.255.255.255
  ```

  Workaround: For all prefixes, configure distances that differ from the distances that were initially configured.

- CSCeh00680

  Symptoms: A router that is configured for Multi-Topology IS-IS (M-ISIS) may reload.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.2S.

  Workaround: Disable M-ISIS.

- CSCsa45381

  Symptoms: CLNS fast-switching is disabled on a serial E3 interface that is configured for HDLC encapsulation.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(30)S but may also occur in other releases.

  Workaround: There is no workaround.

Miscellaneous

- CSCdv07156

  Symptoms: A router that is configured with thousands of RIP routes may crash when multiple links flap.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP.

  Workaround: There is no workaround.

- CSCdx41392

  Symptoms: Please see DDTS CSCdy66662.

  The COPS-PR MIB is no longer part of the Cisco IOS code as of mid-May 2002. All subsequent images do not support this unsupported feature. If an issue is reported against the COPS-PR MIB code, it will not be fixed as this code is no longer supported.

  Results of this caveat (i.e., a router crash during a mibwalk) can be found with either V1 or V2.

Conditions: This caveat will resolve all COPS-PR MIB issues as that code will no longer be present for the Cisco 7200 and Cisco 7500 platform with images listed below:

12.2(08)YW03
12.2(15)BX
12.2(15)ZN
12.2(15)BZ
12.2(10.07)PI05
12.2(10.07)T

All other platforms will have code removed in phase 2 which will be completed in Cisco IOS Release 12.3(05.05)T. Cisco 2600 Routers Fixes are verified in Cisco IOS Release 12.2(15)T7 and Release 12.2(17).

Workaround: To disable the components from CISCO-COPS-CLIENT-MIB, define an SNMP view. Required commands to achieve this are as follows:

```
no snmp-server community <your RO community> RO
snmp-server view no_cops_client internet included
snmp-server view no_cops_client ciscoCopsClientMIB excluded
snmp-server community <your RO community> view no_cops_client RO
snmp-server community <your RW community> view no_cops_client RW
```

- CSCeb37966

  Symptoms: A Cisco 12000 series may reload when you enable Fast Reroute (FRR) on the headend of a tunnel.

  Conditions: This symptom is observed when the tunnel carries Any Transport over Multiprotocol Label Switching (AToM) traffic.

  Workaround: There is no workaround.

- CSCed12234

  Symptoms: A software-forced bus error due to corrupted program counters may occur on a Cisco AS5350.

  Conditions: This symptom is observed on a Cisco AS5350 that runs the C5350-jk9s-m image of Cisco IOS Release 12.3(7)T when a crypto tunnel comes up.

  Workaround: There is no workaround.

- CSCed66010

  Symptoms: The **endpoint max-calls h323id** gatekeeper configuration command works only in one direction.

  Conditions: This symptom is observed on a Cisco platform that functions as a gatekeeper and that runs Cisco IOS Release 12.3(5b) but may also occur in Release 12.3 T. When the limit that is defined in the **endpoint max-calls h323id** gatekeeper configuration command is reached, calls are only restricted via an ARJ message when they are originated at the endpoint that is defined in the **endpoint max-calls h323id** gatekeeper configuration command. Calls that are originated at any other gateway and that are terminated at the gateway that is defined in the **endpoint max-calls h323id** gatekeeper configuration command are not rejected by the gatekeeper via an ARJ message as they should be.

  Workaround: There is no workaround.

- CSCee15145

  Symptoms: A Cisco 3660 that functions as a bridge between ATM media and other interfaces may drop incoming ATM frames.

Conditions: This symptom is observed when PPP over Ethernet (PPPoE) is configured on the ATM PVC on the Cisco 3660.

Workaround: Disable PPPoE on the ATM PVC.

- CSCee32365

  Symptoms: When a single bundle link associated with a Multilink Frame Relay (MFR) interface is brought up, LMI exchanges over the MFR interfaces may not happen.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for MFR.

  Workaround: There is no workaround.

- CSCee32427

  Symptom: A Cisco 2691 may hang after crashing with the following error message:

  ```
  %ERR-1-GT64120 (PCI-0): Fatal error, DMA out of range error
  ```

  Conditions: This symptom is observed when you boot the Cisco 2691.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is only observed on a Cisco 2691.

- CSCee49035

  Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

  Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

  Workaround: There is no workaround.

- CSCee90144

  Symptoms: A gatekeeper may not release or de-allocate the interzone bandwidth correctly. The output of the **show gatekeeper zone status** command shows a non-zero value for the "Current interzone bandwidth" field, even when there are no active calls.

  Conditions: This symptom is observed on a Cisco platform that functions as a gatekeeper and that runs Cisco IOS Release 12.3 in the following topology:

  An H.323 video endpoint connects via a GK/proxy to the gatekeeper that connects to an H.323 central endpoint.

  Calls from the video endpoint are proxied by a Cisco IOS H.323 proxy. This proxy and the gatekeeper are collocated on the same router.

  Workarounds: Enter the **shutdown** gatekeeper configuration command followed by the **no shutdown** gatekeeper configuration command on the gatekeeper to clear the interzone bandwidth.

- CSCef14548

  Symptoms: A Cisco router accepts an incoming plaintext that matches the crypto map that is applied to an interface. The packet should be rejected because is should have been encrypted.

  Conditions: This symptom is observed when all the following conditions occur:

  - The interface is a serial subinterface.
  - The interface has both fast switching and CEF switching disabled.
  - The outgoing interface for the packet has fast switching or CEF switching enabled.

Workaround: Ensure that all interfaces have fast switching and CEF switching either enabled or disabled.

- CSCef28975

  Symptoms: A router that functions as an H.323 gateway crashes.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when authentication is enabled.

  Workaround: Enter the **no memory lite** command.

- CSCef30928

  Symptom: A DHCP server does not add secure ARP entries for DHCP clients that send their initial DHCP request.

  Conditions: This symptom is observed on a DHCP server that assigns IP addresses to DHCP requests that are received on an unnumbered interface.

  Workaround: Use a shorter lease time. Subsequent renewals from the DHCP clients convert the client's ARP entries to secure ones.

- CSCef41501

  Symptoms: The access control entries (ACEs) that are downloaded by the Network Admission Control (NAC) are inserted below the ACEs that are downloaded by the authentication proxy. This situation causes authentication difficulties.

  Conditions: This symptom is observed when both an authentication proxy and NAC are configured on the same interface.

  Workaround: Configure the Cisco ACS server that is used in the configuration in such a way that the authentication proxy does not download any ACEs. Only NAC should install the required ACEs for the session that is being authenticated.

- CSCef44786

  Symptoms: ATM BADVCD error messages are generated and some packet or cell loss is associated with these messages. The cell loss can be observed as MLP fragment loss at the remote end by entering the **show ppp multilink** command.

  Conditions: This symptom is observed on a PA-A3 port adapter that is installed in a FlexWan on a Cisco Catalyst 6500 series that runs a Cisco IOS native software image when MLP over ATM is configured with dLFI on the PA-A3. The symptom occurs only when QoS is configured for dLFIoATM and when the last fragment size is slightly smaller than the number of fragments multiplied by the VC encapsulation size.

  Workaround: You can reduce the chances that the symptom occurs by configure a larger delay, which diminishes the number of fragments.

  Alternate Workaround: If this an option, configure the PVC at 192 kbps or a higher bandwidth, which also ensures large fragment sizes.

- CSCef67842

  Symptoms: Router may not be able to detect busy and congestion on Japan cptone.

  Conditions: This symptom is observed on a Cisco 2600, Cisco 3640, and Cisco 3660.

  Workaround: There is no workaround.

- CSCef87827

  Symptoms: IP routes that are inserted by DHCP are not removed from the routing table, and the tracked object goes down.

Conditions: This symptom is observed when you enter the **ip dhcp client route track** *object* command. DHCP removes the 0.0.0.0/0 route but not any static routes that use the **dhcp** keyword for the IP next-hop address, even though DHCP adds both the 0.0.0.0/0 route and these static routes to the routing table.

Workaround: There is no workaround.

- CSCef94974

  Symptoms: A Cisco 7200 series that functions as a gateway GPRS support node (GGSN) may crash randomly while forwarding traffic.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(8)T4 under normal operating conditions.

  Workaround: There is no workaround.

- CSCef96035

  Symptoms: All IPSec sessions may be dropped from a Cisco 7200 series and the router generates the following error messages continuously:

  ```
  %VPN_HW-1-ERROR: slot: 2 - ENOSPACE tx cmd 2 ring. Head 83, Tail 82, Used 255, buf 0
  IPSECcard: an error coming back 0x1510
  ```

  Other symptoms that may occur during this time include the following:

  - High CPU utilization during the “Crypto Delete Manager” process.
  - An I/O memory allocation failure during the “Crypto Delete Manager” process.

  Conditions: This symptom is observed on a Cisco 7200 series that is equipped with two VPN acceleration modules (SA-VAMs) that are configured for VRF-aware IPSec.

  Workaround: There is no workaround. To temporarily clear the symptoms, reload the router.

- CSCef97768

  Symptoms: A PCMCIA flash card that is installed in either slot 0 or slot 1 of a Cisco 3620 may become read-only.

  Conditions: This symptom is observed occasionally on a Cisco 3620 that runs Cisco IOS Release 12.3(6b).

  Workaround: There is no workaround.

- CSCeg01543

  Symptoms: A Cisco 7500 series VIP may crash when its serial interfaces are part of a Multipoint Frame Relay (MFR) bundle.

  Conditions: This symptom is observed when a Frame Relay end-to-end fragment is received on an MFR interface.

  Workaround: Administratively shut down the MFR interface or shut down the MFR interface on the other side of the link.

- CSCeg06220

  Symptoms: An EZVPN tunnel does not come up and becomes stuck in the “VALID_CFG” state even though the tunnel is configured to come up automatically.

  Conditions: This symptom is observed on a router that is rebooted with EZVPN enabled on an interface.

  Workaround: Unconfigure and reconfigure EZVPN on the interface.

- CSCeg07394

  Symptoms: The router pauses indefinitely at startup.

  Conditions: This symptom is a side effect of the fix for CSCee81074. This symptom has been observed occasionally when the router is booting up. The symptom is in the memory allocation portion of the TCL component. If the image does not contain any components using TCL, this symptom will not occur.

  Workaround: Do not use an image that contains TCL components, otherwise, there is no workaround.

- CSCeg12134

  Symptoms: When you send multicast traffic over an IPSec tunnel, a memory leak may occur on a router.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when both IP CEF and hardware encryption are configured.

  Workaround: Switch to software encryption for a while and then switch back to hardware encryption.

  Alternate Workaround: Disable IP CEF.

- CSCeg15000

  Symptoms: Modem relay over TCCS works fine when you save the configuration and reload the router. However, a modem call goes into pass-through mode when you enter the **shutdown** voice-port configuration command followed by the **no shutdown** voice-port configuration command on the trunked voice port.

  Conditions: This symptom is observed on a Cisco 3700 series that functions as a voice gateway.

  Workaround: After the router has booted, do not enter the **shutdown** voice-port configuration command followed by the **no shutdown** voice-port configuration command on the trunked voice port.

- CSCeg15065

  Symptoms: After a DSP restarts, RTP packets are not sent from the DSP to a trunk connection.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that runs Cisco IOS Release 12.3(10a) or Release 12.3(11)T when the **connection trunk** command is enabled.

  Workaround: There is no workaround. To re-enable the DSP to send RTP packets, enter the enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the voice port that is associated with the DSP.

- CSCeg15855

  Symptoms: Hairpinned calls fail.

  Conditions: This symptom is observed on a Cisco router that is configured with an NM-HDV2-2T1/E1 network module.

  Workaround: There is no workaround.

- CSCeg15922

  Symptoms: A DMVPN tunnel (mGRE) may not fully initialize at startup. When you enter the **no shutdown** command on the tunnel interface, the platform may crash with a "tunnel_protection_setup_socket" error.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2SX but may also occur in Release 12.3 or Release 12.3T.

Workaround: Create a point-to-point GRE tunnel on the spokes (instead of via mGRE) and an mGRE tunnel on the hub. Note that you need an NHRP Next Hop Server (NHS) configuration in order for the hub to learn the spokes.

Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface in order for the tunnel to come up. However, after you have implemented the Alternate Workaround, the crash may still occur.

Further Problem Description: The crash occurs only on a spoke router or spoke switch, not on a hub router or hub switch. Furthermore, the crash is only observed on a Cisco Catalyst 6000 series and a Cisco 7600 series and may occur with any DMVPN configuration that uses mGRE tunnels.

- CSCeg17082

  Symptoms: All voice calls fail and the output of the **show voice port summary** command shows that all voice ports are in the down state:

```
                                        IN       OUT
PORT      CH   SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
========= == ============ ===== ==== ======== ======== ==
0/1:0     01  e&m-wnk     up    down idle     idle     y
0/1:1     02  e&m-wnk     up    down idle     idle     y
0/1:2     03  e&m-wnk     up    down idle     idle     y
```

  Conditions: This symptom is observed on a Cisco 2600 series, Cisco 3660, and Cisco 3700 series that run Cisco IOS Release 12.3(11)T1 or Release 12.3(11)T2 and that are configured with an AIM-VOICE interface module that has DSPs that are configured for high complexity. The symptom occurs after you reload the router.

  Workaround for Release 12.3(11)T1: Bring the voice ports to the up state by entering the **shutdown** voice-port configuration command followed by the **no shutdown** voice-port configuration command on the affected voice ports.

  Workaround for Release 12.3(11)T2: Remove the affected DS0 group and reconfigure it.

- CSCeg20412

  Symptoms: A router may not properly detect supervisory tones.

  Conditions: This symptom is observed on a Cisco 3640 and Cisco 3660 only when a DSP is configured to detect custom cptones and when no cadence is specified for the tone. The symptom may also occur on other routers.

  Workaround: There is no workaround.

- CSCeg20777

  Symptoms: A router may crash while handling secure HTTP (HTTPS) traffic, and the following traceback is generated:

```
-Traceback= 607C675C 61DAC154 61DAC258 61DBAFC4 61DC2BB4 61E1F6E4 609AFEDC
607B3
FD4 607B3FB8
$0 : 00000000, AT : 80000000, v0 : 00000000, v1 : 00000000
a0 : 62200000, a1 : 647EF1D0, a2 : 0000004E, a3 : 647FD2AC
t0 : 00000001, t1 : 00000000, t2 : FFFFFFFF, t3 : 00000000
t4 : 6D312730, t5 : 864886F7, t6 : 16187A72, t7 : 2D30312E
```

```
s0 : 6480B404, s1 : 0D0D0CE5, s2 : 0000004E, s3 : 0000004E
s4 : 0D0D0D0D, s5 : 647FD2AC, s6 : 64811470, s7 : 00000000
t8 : 647CAED8, t9 : 00000000, k0 : 3040D001, k1 : 00000000
gp : 631F6D08, sp : 64811318, s8 : 63C8B8B8, ra : 607C6738
EPC  : 607C675C, ErrorEPC : 33B3723E, SREG     : 3400FF03
MDLO : 00000009, MDHI     : 065FFC90, BadVaddr : 0D0D0D0B
Cause 00000010 (Code 0x4): Address Error (load or instruction fetch) exception
```

Conditions: This symptom is observed on a Cisco router that has Public-Key Infrastructure (PKI) configured.

Workaround: There is no workaround.

- CSCeg21929

  Symptoms: Voice packets are not compressed when cRTP is configured with MQC on a serial interface that is configured for Frame Relay encapsulation.

  Conditions: This symptom is observed on a Cisco 3725, Cisco 3745, and Cisco 7206.

  Workaround: Disable CEF globally and disable fast switching on the serial interface.

- CSCeg23176

  Symptoms: A Cisco RPM-XF is reset by the PXM because of an SCM poll timeout. A PCI information file is generated in the bootflash memory just before the Cisco RPM-XF resets.

  Conditions: This symptom is observed when a PCI error interrupt occurs along with SDRAM parity errors that are continuously serviced.

  Workaround: There is no workaround.

- CSCeg26669

  Symptoms: Pre-emption of a low-priority voice call does not occur when a higher-priority voice call is placed using an MLP prefix string.

  Conditions: This symptom is observed when voice calls are placed through a T1 CAS connection.

  Workaround: There is no workaround.

- CSCeg27043

  Symptoms: PIM neighbors continue to flap after you have reloaded microcode.

  Conditions: This symptom is observed on a Cisco MGX 8850 series RPM-XF that runs Cisco IOS Release 12.3T.

  Workaround: Enter the **clear ip mroute *** command to clear the symptoms.

- CSCeg28309

  Symptoms: The **max-users** *number-of-users* and the **max-logins** *number-of-users* command do not function in an HA environment.

  Conditions: This symptom is observed on a Cisco platform that runs a Cisco IOS release later than Release 12.3(4)T9 and that is configured for HA.

  Workaround: There is no workaround.

- CSCeg31430

  Symptoms: A memory leak may occur on a router that has rate-limiting configured.

  Conditions: This symptom is observed when the router is configured with two mutually exclusive exceed statements as in the following example:

  ```
  Router#sh run | b <name>
  ```

```
policy-map <name>
   class <classname>
     bandwidth 50
     random-detect
     random-detect exponential-weighting-constant 3
     random-detect precedence 0 3 9 1
     random-detect precedence 7 3 11 1
    police cir 50000 bc 8000 pir 119000 be 16000
      conform-action transmit
      exceed-action transmit
      exceed-action set-prec-transmit 0
      violate-action drop
     queue-limit 22
```

Workaround: To stop the memory leak, delete one of the exceed statements.

- CSCeg35786

  Symptoms: 20 percent of received faxes fails. Faxes arrive either partially, as a compressed page, or as invalid TIFF files.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(7)T when the T.37 Store and Forward Fax feature is configured and when the faxes are received by a mail server that is connected to the Cisco AS5850.

  Workaround: There is no workaround.

- CSCeg38482

  Symptoms: AutoRP packets are dropped because of an RPF failure.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when both the Candidate RP and Mapping Agent (MA) are configured in a VRF context and when the interface is not specified in the **ip pim vrf** *vrf-name* **send-rp-discovery** *interface-type interface-number* command. This situation may cause the MDT update source address (an address that belongs to the global table) for the MVPN to be chosen and, in turn, the AutoRP flow to be created in the downstream route with a global address as the source.

  Workaround: Configure the interface that has the highest IP address in the VPN as the Candidate RP and MA.

  Alternate Workaround: Configure the interface that is defined in the Candidate RP as the interface in the **ip pim vrf** *vrf-name* **send-rp-discovery** *interface-type interface-number* command.

- CSCeg39560

  Symptoms: After a router is rebooted, a tunnel interface does not acquire the IP address of the async serial interface that is the tunnel source.

  Conditions: This symptom is observed on a Cisco 2600 series that runs Cisco IOS Release 12.3(8)T3.

  Workaround: Enter the **tunnel source interface-type** *interface-number* command on the tunnel interface.

- CSCeg40721

  Symptoms: Tail drops are seen on SAR CoS queues in XFL PEs.

Conditions: This symptom occurs when SAR-based QoS is configured and bursty traffic is sent on VCs with output policy-maps configured on them.

Workaround: Depending on the size of the bursts, increasing queue size may help absorb it. It is to be understood that this can increase delay and if used on many VCs, can significantly increase buffer usage.

- CSCeg47213

  Symptoms: A router may crash when a PPPoA subinterface is removed.

  Conditions: This symptom is observed when many PPPoA sessions are in transition.

  Workaround: Shut down the subinterface, clear all the PPPoA sessions, verify that all the sessions are cleared, and then remove the subinterface.

- CSCeg50001

  Symptoms: Upstream traffic does not reach a public data network (PDN), and the send and receive counters are incremented properly.

  Conditions: This symptom is observed when you send process-switched packets upstream over a packet data protocol (PDP) link in a GPRS network.

  Workaround: There is no workaround.

- CSCeg50651

  Symptoms: When a router has the **moh-live** *dn-number out-call* command enabled with 1234 for the *dn-number* argument and 9876 for the *out-call* argument, the outcall to an FXO port does not occur. Only when the router is manually placed into SRST mode does the outcall occur.

  Conditions: This symptom is observed on a Cisco 2800 series that is configured as a MGCP gateway.

  Workaround: Place the gateway into SRST mode, force the outcall to the live feed, then place the router back into MGCP mode.

  Further Problem Description: This caveat is an enhancement to the MOH Live-Feed Support feature. The fix for this caveat ensures that MoH works in any configuration, not only when the router functions in SRST mode.

- CSCeg51793

  Symptoms: When you delete an IP VRF by entering the **no ip vrf** *vrf-name* command and you attempt to reconfigure the IP VRF before it is completely deleted, an address error exception may occur.

  Conditions: This symptom is observed on a Cisco platform that is configured for MVPN.

  Workaround: Wait until the IP VRF is completely deleted: enter the **show ip vrf** command to verify that the IP VRF is deleted before you reconfigure it.

- CSCeg53483

  Symptoms: When you enter the **show running-config** command, a traceback may be generated because of a CPU hog condition.

  Conditions: This symptom is observed when large number of class maps (2500) is configured.

  Workaround: There is no workaround.

- CSCeg53889

  Symptoms: The HTTP client does not check the file size limit for streaming files before caching them.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(9a), that functions as a voice gateway and voice browser in an Internet Service Node (ISN) solution, and that is configured for VXML.

Workaround: There is no workaround.

- CSCeg54615

  Symptoms: There may be a large latency in responding to EAPoUDP events from a host, causing the idle timer to expire and network access for users to be delayed.

  Conditions: This symptom is observed on a Cisco router that is configured for Network Admission Control (NAC).

  Workaround: There is no workaround.

- CSCeg55584

  Symptoms: A Cisco router that is configured for PPPoE may stop forwarding packets that need to be fragmented.

  Conditions: This symptom is observed after a link flap occurs on the dialer interface or after you enter the **clear interface** command on the dialer interface.

  To re-enable the affected packets to be forwarded, enter the **no ip cef** command followed by the **ip cef** command.

  Possible Workaround: Enter the **ip tcp adjust-mss 1400** command to force the maximum segment size (MSS) of the TCP SYN packets to be small enough to prevent the router from fragmenting the packets.

- CSCeg57219

  Symptoms: On a Cisco 7600 router, packets with certain packet sizes may fail to ping on RPR+ switchover or interface flap on a multilink interface with members from non-channelized PAs when multilink interface is configured with fragmentation and interleaving.

  Conditions: This symptom might happen on RPR+ switchover or link flap.

  Workaround: There is no workaround.

- CSCeg59923

  Symptoms: The following error message is generated during a voice stress test:

  ```
  %DSM-3-DSP_TIMEOUT: DSP timeout on channel
  ```

  Conditions: This is symptom is observed on a Cisco AS5850.

  Workaround: There is no workaround.

- CSCeg61162

  Symptoms: Caller ID presentation does not function because a Cisco VG224 does not reverse the line polarity.

  Conditions: This symptom is observed on a Cisco VG224 that has the **caller-id alerting line-reversal** command enabled.

  Workaround: There is no workaround.

- CSCeg61586

  Symptoms: A router may reload when PPPoA sessions are being established or torn down.

  Conditions: This symptom is observed when the configuration of the ATM interface over which the sessions are received is altered.

  Workaround: There is no workaround.

- CSCeg62088

  Symptoms: A Cisco voice gateway may reload unexpectedly because of a bus error, pointing to an invalid address.

  Conditions: This symptom is observed on a Cisco AS5350 and Cisco AS5400 that run Cisco IOS interim Release 12.3(12.5).

  Workaround: There is no workaround.

- CSCeg63430

  Symptoms: One-way voice occurs when an IP phone transfers a call back to the PSTN via a Cisco AS5850 after having received the call from the PSTN via the same Cisco AS5400. The caller at the PSTN side hears the transferee at the (other) PSTN side, but not the other way around.

  Conditions: This symptom is observed when the Cisco AS5850, which runs Cisco IOS Release 12.3T, connects to the PSTN via an PRI in the following topology:

  ```
  Caller--Phone--PSTN--PRI--AS5850--CCM--IP Phone Transfer--CCM--AS5850--PRI--
  PSTN--Transferee
  ```

  Workaround: Enable MTP or the Cisco CallManager.

  Further Problem Description: Although the symptom is not observed in Cisco IOS Release 12.3, the fix is included in Cisco IOS Release 12.3 as a precaution.

- CSCeg64074

  Symptoms: A switch connection fails when created with SCR at the OC24 rate (1197656 kbps).

  Conditions: This symptom has been observed when creating a switch connection between two XF cards with service type vbr-nrt and SCR/PCR at the OC24 rate.

  Workaround: Use a switch connection with at least 1kbps less than the OC24 rate.

- CSCeg64669

  Symptoms: A Cisco AS5850 reloads when it fetches a TDM connection object for a TDM hairpinned call. while handing over peer resources to the standby RSC.

  Conditions: This symptom is observed when you enter the **redundancy handover peer-resource** command and when the Cisco AS5850 functions in the extra-load state.

  Workaround: Clear all existing calls that use peer resources and mark the calls as busyout before you enter the **redundancy handover peer-resource** command.

- CSCeg64679

  Symptoms: A Cisco AS5850 reloads when you enter the **redundancy handover peer-resources** command to hand over the peer resources to the other RSC.

  Conditions: This symptom is observed when the RSC that hands over the peer resources is in the "ACTIVE_EXTRALOAD" mode and when an SNMP trap is sent to obtain the card status.

  Workaround: There is no workaround.

- CSCeg66282

  Symptoms: The controller of a 1-port multichannel STM-1 port adapter (PA-MC-STM1) does not come up after the router has reloaded.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S2. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg66913

  Symptoms: A router may crash during a modem firmware upgrade.

  Conditions: This symptom is observed when modem calls are still up and when modem debugging is enabled.

  Workaround: Disable all debugs.

- CSCeg72444

  Symptoms: A router that is configured for SSG may hang and crash.

  Conditions: This symptom is observed when PBHK and idle timeout are enabled for PPP users and the router is busy.

  Workaround: Disable idle timeout for all PPP users.

  Alternate Workaround: Disable PBHK. If you do so, you may still observe a few non-aligned accesses but a crash will not occur.

- CSCeg73626

  Symptoms: A DSP farm profile cannot be configured.

  Conditions: This symptom is observed on a Cisco 3700 series and Cisco 3800 series when a voice card does not have the **dsp services dspfarm** command enabled.

  Workaround: Enter the **dsp services dspfarm** command on at least one voice card.

- CSCeg76294

  Symptoms: A gateway that has a higher IP address in comparison with its peer may fail to open a TCP connection for a logical channel.

  Conditions: This symptom is observed during fast start when a glare condition occurs while both gateways indicate to each other (in facility or other H.225 messages) that the H.245 control channel should be opened.

  Workaround: There is no workaround.

- CSCeg77587

  Symptoms: Calls via a V.110 L2TP GSM application fail.

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.3(2)T or a later release and that is configured for MGCP NAS. Debugs show PPP and CRC errors and corrupt asynchronous framing.

  Workaround: There is no workaround.

- CSCeg78279

  Symptoms: A Cisco Catalyst 6500 series Communication Media Module (WS-CMM-SVC) may crash frequently.

  Conditions: This symptom is observed on a Catalyst 6509 that is configured with a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD2 while the WS-CMM-SVC runs Release 12.3(8)XY2. The symptom may also occur in Release 12.3T.

  Workaround: There is no workaround.

- CSCeg78427

  Symptoms: High CPU utilization may occur on a Cisco 2600XM that is configured for Circuit Emulation over IP (CeoIP). When you enter a command such as the **show running-config** or the **show tech-support** command, the overrrun counter and underrun counter in the output of the **show cem** *slot/port/channel* command increases and frames are lost.

Conditions: This symptom is observed when data is sent from a BERT tester to a Circuit Emulation over IP network nodule that is installed in a Cisco 2600XM that connects via an Ethernet link to another Circuit Emulation over IP network nodule that is installed in another Cisco 2600XM.

Workaround: There is no workaround.

- CSCeg78458

  Symptoms: A Cisco 836 or Cisco 837 may reload because of a software-forced crash when you request a reload with an XML file via CNS.

  Conditions: This symptom is observed with a CNS Configuration Engine version 1.4 that runs on an IE2115 server. The routers run Cisco IOS Release 12.3(8)YG. The symptom could also occur in Release 12.3.

  Possible Workaround: Enter the **scheduler max-task-time 50000** command.

- CSCeg78674

  Symptoms: When you download a Cisco IOS image from CNS via an XML file to a Cisco 836 or Cisco 837, meaningless characters are generated on the router console and an invalid memory action with an associated traceback is generated on the CNS event bus.

  Conditions: This symptom is observed with a CNS Configuration Engine version 1.4 that runs on an IE2115 server. The routers run Cisco IOS Release 12.3(8)YG. The symptom could also occur in Release 12.3.

  Workaround: Enter the **no logging cns-events** command on the router. This command is enabled by default.

- CSCeg79652

  Symptoms: When you enter the **reload** command on a router that is configured with an SHDSLv2 card, the router enters an endless loop.

  Conditions: This symptom is observed only with SHDSLv2 cards on a Cisco router that runs a Cisco IOS Release later than interim Release 12.3(12.6)T.

  Workaround: To recover the router from the loop, enter the **send brk** command to enable the router to enter ROMmon mode.

- CSCeg79821

  Symptoms: A Cisco 7200 VXR router crashes after running out of I/O memory because of a buffer leak in a public particle pool.

  Conditions: This symptom is observed on a 7200 VXR router that runs Cisco IOS Release 12.3(9c) or Release 12.3(12) and that is configured with an NPE-G1. The symptom does not occur in Release 12.3(9).

  Workaround: There is no workaround.

- CSCeg80858

  Symptoms: When the buffered calling name functionality is enabled, calls from an ISDN gateway to a SIP device do not reflect correct screening and presentation indicators (as set in Octect3A by the originating switch) in the Remote-Party-Id header of an outgoing INVITE message. In addition, the gateway does not include the calling number in the Remote-Party-Id.

  Conditions: This symptom is observed for calls that come from the PSTN via an ISDN gateway to a SIP device when the buffered calling name functionality is enabled so that the gateway has to wait for an ISDN FACILITY message for the calling name information before it can send an INVITE message.

  Workaround: Disable the buffered calling name functionality.

- CSCeg81698

  Symptoms: After a DSP crashes and recovers, voice calls through a backhauled PRI fail. Note that a regular PRI is not affected.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(8)T6, that functions as a voice gateway, and that is configured with an NM-HDV2 and a PVDMII-24.

  Workaround: Enter the **shutdown** voice-port configuration command followed by the **no shutdown** voice-port configuration command on the affected voice port. Note that shutting down and bringing up the controller on the affected voice port does not bring the voice port back up.

- CSCeg81870

  Symptoms: In SRST mode, a phone does not completely register with a voice gateway, preventing SRST from functioning.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(11)T3 when a service URL is associated with speed buttons.

  Workaround: There is no workaround.

- CSCeg82392

  Symptoms: A Cisco CallManager uses different versions of the G.729 codec when setting up Message Transfer Protocol (MTP) calls across intercluster trunks. The Cisco CallManager should set up the call legs with the same versions of the G.729 codec.

  Conditions: This symptom is observed when a Cisco 3700 series that runs Cisco IOS Release 12.3(11)T2 connects to a Cisco CallManager that runs version 4.1.

  Workaround: There is no workaround.

- CSCeg82614

  Symptoms: A memory leak may occur in the in the “CCH323_CT” and “VTSP” processes.

  Conditions: This symptom is observed on a Cisco 3660 that is configured for AAA.

  Workaround: There is no workaround.

- CSCeg82704

  Symptoms: When a phone call is made and forwarded to a Cisco Unity Express Network Module (NM-CUE), choppy voice may occur on the IP phone(s) that are connected to the stacked Etherswitch modules. The symptom is observed for voice connections between the IP-phone(s) and the NM-CUE. The sound during calls between two IP phones is good.

  Conditions: This symptom is observed when a 16-port Etherswitch module is stacked with a 36-port Etherswitch network module. This symptom does not occur when only a single Etherswitch module (either 16- or 36-port) is used.

  Workaround: There is no workaround.

- CSCeg84573

  Symptoms: Traffic, including cell-based MPLS traffic, may be affected (that is, traffic may be dropped, or its behavior may be modified) after you have modified a QoS policy map that is already attached to an interface by way of adding a new class or deleting an existing class.

  Additionally, when a cell-based interface is affected by the above-mentioned symptom, traffic on other switch subinterfaces may also be affected even though the same policy map is not applied to these subinterfaces.

  Conditions: These symptoms are observed on when the following conditions are present:

  – A policy map “p” is configured with more than class.

  - A particular class “y” is removed from “p” explicitly through the **no class y** command or implicitly by removing all the class-map actions under class “y”.
  - For all classes under “p”, including the “class-default” that is configured for “police” and that follows class “y” prior to its removal, the matching traffic is treated with the “exceed” action.

  Workaround: To prevent the symptoms form occurring: enter the **shutdown** command on the interface before you modify the policy map. Enter the **no shutdown** command after you have modified the policy map.

  Alternate Workaround: When the symptom has occurred and the interface is already affected, enter the **shutdown** command followed by the **no shutdown** command on all affected subinterfaces.

- CSCeg85709

  Symptoms: A fax to or from an FXS port does not go through as modem pass-through.

  Conditions: The symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(12.12)T1 when modem pass-through is configured globally.

  Workaround: There is no workaround.

- CSCeg86251

  Symptoms: The CISCO-CDP-MIB is missing.

  Conditions: This symptom is observed only on a Cisco 831.

  Workaround: There is no workaround.

- CSCeg87507

  Symptoms: DSP programming on a router fails, causing a BRI call to disconnect. The output of the **debug voip vtsp session** command shows “DSP programming failed”.

  Conditions This symptom is observed on a Cisco 2800 series, Cisco 3800 series, and any other router that uses Flex DSP resource management (DSPRM) when calls are made from a BRI or PRI to the PSTN and when the PSTN side sends a Call Proc message followed by a Call Alerting message.

  Workaround: There is no workaround.

- CSCeg87892

  Symptoms: VIPs crash when GRE tunnels are configured in an MPLS VPN configuration. The interface names are not displayed in the output of the **show adjacency detail** command output because the name strings of the FIBIDBs are incorrectly allocated.

  Conditions: These symptoms are observed when GRE tunnels are configured on MPLS PE routers. However, the incorrect allocation of the name strings of the FIBIDBs may occur on any platform.

  Workaround: There is no workaround.

- CSCeh00270

  Symptoms: A Cisco gateway may reload at “h245_olc_out_sm”.

  Conditions: This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.3(7)T7 when the gateway receives a third-party RequestChannelClose message that has the reason field populated with “reopen”.

  Workaround: Ensure that the third-party gateway does not send a RequestChannelClose message with the reason field populated with “normal”.

- CSCeh01182

  Symptoms: A Cisco voice gateway may drop a voice or fax relay call during CNG tone detection.

Conditions: This symptom is observed on a Cisco voice gateway that is configured with a VXML application script on the incoming POTS dial peer and that receives a fax CNG tone.

Workaround: There is no workaround. However, this is the limitation on voice gateways that use VXML applications: such platforms only support T.37.

Further Problem Description: The fix for this caveat includes support for T.38 on voice gateways that use VXML applications.

- CSCeh02312

  Symptoms: A router may reload when you lock or unlock an RSA key pair.

  Conditions: This symptom is observed when you enter the **crypto key lock rsa passphrase** *passphrase* or **crypto key unlock rsa passphrase** *passphrase* EXEC command.

  Workaround: Do not include the **passphrase** keyword and associated argument in the command. Neither include the optional **name** keyword and the associated *key-name* argument in the command because the router prompts for key name that you want to lock or unlock.

- CSCeh03945

  Symptoms: When you reload a router, its BRI interface configuration is modified.

  Conditions: This symptom is observed on a Cisco 1760.

  Before you reload the router, the configuration of the BRI interface is as follows:

```
interface BRI0/0
 no ip address
 isdn switch-type basic-net3
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager service mgcp
 isdn send-alerting
 isdn static-tei 0
 isdn skipsend-idverify
```

  After you have reloaded the router, the configuration of the BRI interface is as follows:

```
interface BRI0/0
 no ip address
 isdn switch-type basic-net3
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn send-alerting
 isdn static-tei 0
 isdn skipsend-idverify
```

  Note that the **isdn bind-l3 ccm-manager service mgcp** command is now deleted.

  Workaround: There is no workaround.

- CSCeh05540

  Symptoms: Packet statistics that are displayed under an L2 policy map are incorrect. The counters that show incorrect information are the “Conformed packets/bytes” and “Exceeded packets/bytes” counters.

Conditions: This symptom is observed on a Cisco MGX RPM-XF when a policy map is applied to any of its interfaces and when the affected counters cross the actual value of 4294967295.

Workaround: There is no workaround.

- CSCeh06200

  Symptoms: Administrators are unable to gain access via HTTP if idle time is set on TACACS server. Telnet via TACACS works as expected.

  Conditions: This symptom has been observed with TACACS configured on the AP.

  Workaround: There is no workaround.

- CSCeh06736

  Symptoms: When IP header compression is enabled on a PPPoATM or PPPoFR interface, compressed packets are not correctly classified by any QoS policy that has been applied to the supporting ATM or Frame Relay PVC.

  Conditions: This symptom is observed when CRTP is enabled on the virtual-template interface via the **service policy** command or **ip rtp header-compression** command and when the IP RTP Priority feature is enabled in the PVC policy.

  Workaround: There is no workaround.

- CSCeh06778

  Symptoms: If a default route is redistributed from RIP into BGP, then back into RIP on another router, the default route is not marked as poisoned or withdrawn on the CE router that receives the updates.

  Conditions: This symptom is observed when a CE router sends the default route via RIP to a PE router, when the PE router advertises this route to a second CE router, and when the link between the first CE router and the PE router is disconnected.

  Workaround: There is no workaround.

- CSCeh10646

  Symptoms: A router may unexpectedly reloads because of a bus error at an address that falls just short of the I/O memory range such as address 0x4E7FD5B8, whereas the iomem address starts at 0x4E800000.

  Conditions: This symptom is observed when the router has some of the following security feature commands enabled on one or more interfaces:

  ```
  ip nbar protocol-discovery
  ip virtual-reassembly
  ip access-group in
  ip access-group out
  ip inspect in
  ip inspect out
  ip ips in
  ip ips out
  auto discovery qos
  crypto map
  ```

  Workaround: Remove the **ip access-group out** command.

- CSCeh10980

  Symptoms: A Cisco voice gateway may reload when a consultation call transfer is executed using a default session application.

  Conditions: This symptom is observed on a Cisco voice gateway that is configured for IVR.

  Workaround: There is no workaround.

- CSCeh12839

  Symptoms: A SSG does not return GPRS VSAs to a GGSN in an access-accept message.

  Conditions: This symptom is observed when a RADIUS client such as a GGSN sends an extended auto-domain access request. The SSG should return the “gprs:charging-profile-index” and “csg:billing_plan” VSAs in the auto-domain profile to the GGSN when the **no remove vsa cisco** command is enabled on the SSG for the RADIUS client.

  Workaround: There is no workaround.

- CSCeh13450

  Symptoms: When you enter the **show controllers** command on a Cisco 3xxx series router, the router either reloads because of a watchdog timeout or hangs. Note that the **show controllers** command is also part of the **show technical-support** command.

  Even with the configuration register set to allow a break into rommon (0x2002), this facility remains unavailable when the router hangs. If this situation occurs, you must power-cycle the router to bring it up.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  – The router has an NM-16A network module installed.

  – The router is configured with one or more async interfaces that are configured on the NM-16A network module.

  Workaround: There is no workaround.

- CSCeh19106

  Symptoms: A Service Selection Gateway (SSG) that is deployed in a GPRS access environment and that is configured for L2TP tunnel service with an extended autodomain may reload when duplicate GPRS PDP context create requests are sent.

  Conditions: This symptom is observed when the PDP context create requests contain the static addressing, that is, the IP address of the MS instead of all zeros in the end user address field.

  Workaround: There is no workaround. Note that for corporate access through a GPRS access-based solution using SSG, generally dynamic addressing is used. With dynamic addressing, the end-user address field is sent with all zeros and the corporate network provides the address, and the symptom does not occur.

- CSCeh21613

  Symptoms: When multicast is configured as part of a dial-peer configuration and you enter the **shutdown** command quickly followed by the **no shutdown** command on a voice port that is part of the dial-peer configuration, the router may generate tracebacks and may crash.

  Conditions: This symptom is observed on a Cisco 1760 that runs Cisco IOS Release 12.3(11)T4.

  Workaround: There is no workaround.

- CSCeh21680

  Symptoms: A Cisco 2800 series or Cisco 3800 series may crash when you configure the interface of an NM-16ESW.

Conditions: This symptom is observed when you enter the **ip rsvp bandwidth** command on FE port 1/10 of the NM-16ESW and then you enter the **no switchport mode** command followed by the **switchport mode** command.

Workaround: Do not enter IP commands in switchport mode.

- CSCeh22179

  Symptoms: No traffic is sent from a Cisco 3825.

  Conditions: This symptom is observed on a Cisco 3825 that runs Cisco IOS Release 12.3(11)T3 when traffic from a VPN that leaves through the global interface does not require encryption.

  Workaround: Remove the crypto map from the global interface.

- CSCeh23047

  Symptoms: After a manual SSO switchover, traffic in the tag switching-to-IP switching direction between an egress 1-port 10-Gigabit Ethernet Engine 4+ line card and an ingress 4-port Gigabit Ethernet ISE line card does not recover.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.

  Workaround: Reload microcode onto the 4-port Gigabit Ethernet ISE line card.

- CSCeh24075

  Symptoms: Packets that are larger than 4400 bytes or packets that require fragmentation may be dropped when they traverses a xDSL WIC.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(6)T or a later release when a sweep ping is performed from one peer to another and when the WIC is a WIC-1ADSL, WIC-1ADSL-DG, WIC-1ADSL-I-DG, WIC-SHDSL, or WIC-SHDSL-V2.

  Workaround: Avoid fragmentation on the DSL link or enter the **ip mtu** *bytes* command to change the maximum MTU to 4400 on the DSL interface.

- CSCeh24202

  Symptoms: A Cisco 2800 series that is configured for software or hardware encryption and CBAC may reload.

  Conditions: This symptom is observed when IPSec SAs and CBAC sessions are established and when the traffic is blocked by an ACL on the outgoing WAN interface of a neighboring crypto router. When you send encrypted traffic from the neighboring crypto router to another router via the Cisco 2800 series, the Cisco 2800 series reloads.

  Workaround: Permit the encrypted traffic on the outgoing interface of the neighboring crypto router.

- CSCeh24815

  Symptoms: High CPU utilization occurs on a Cisco AS5850.

  Conditions: This symptom is observed on a Cisco AS5850 that runs Cisco IOS Release 12.3(11)T3 when dCEF is not applied to packets because of a slow start configuration.

  Workaround: Remove the slow start configuration.

- CSCeh25446

  Symptoms: The following error message may be generated when a Cisco AS5850 voice gateway boots:

  ```
  Could not enable MAC
  ```

  This situation may prevent line cards from booting up and pings over the Fast Ethernet and Gigabit Ethernet interfaces may fail.

Conditions: This symptom is observed on a Cisco AS5850 voice gateway that runs Cisco IOS Release 12.3T.

Workaround: There is no workaround.

- CSCeh25459

  Symptoms: A call fails when the codec is changed from G.729 to G.711ulaw during the call.

  Conditions: This symptom is observed when fax pass-through is configured and when the following events occur:

  - The initial codec for the call is negotiated as G.729.
  - A reinvite message with a codec change to G.711ulaw is sent to the gateway.
  - The gateway accepts the change with a 200 OK message but continues to send the call with codec G.729 in the RTP stream.

  Workaround: Remove the fax pass-through configuration.

- CSCeh31306

  Symptoms: A Cisco MGX RPM-PR does not boot up.

  Conditions: This symptom is observed when the Cisco MGX RPM-PR does not receive the boot acknowledgement from the PXM.

  Workaround: There is no workaround.

- CSCeh34089

  Symptoms: You cannot run the Embedded Event Manager Tcl policy scripts.

  Conditions: This symptom is observed in all Cisco IOS software images that contain the fix for caveat CSCeg07394. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07394. 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.

- CSCeh35434

  Symptoms: An Embedded Event Manager TCL policy does not function.

  Conditions: This symptom is observed on a Cisco IOS software image that contains the fix for caveat CSCeg07394. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07394. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCeh37039

  Symptoms: A file system fails to complete the **dir** command or a **show** command upon encountering a unrecognized file.

  Conditions: This symptom is observed when there is a file of a type that is unrecognizable or not supported by the USB token file system.

  Workaround: Format the USB token prior to its first use.

- CSCeh41997

  Symptoms: EEM Tcl policies leak a significant amount of memory every time they run.

Conditions: This symptom occurs because the memory model that is currently implemented in Cisco IOS software that supports Tcl assumes a single threaded model in which global memory is not released when the Tcl script completes.

Workaround: There is no workaround.

- CSCeh50570

  Symptoms: A Cisco platform reloads when bringing up bulk async and digital SS7/vpdn calls.

  Conditions: This symptom is observed on the Cisco AS5850 platform.

  Workaround: There is no workaround.

- CSCin78987

  Symptoms: A Cisco 3660 shows fluctuations in the CPU utilization and the CPU useage peaks frequently at 100 percent, as you can observe in the output of the **show processes cpu** command.

  Conditions: This symptom is observed on a Cisco 3660 that runs Cisco IOS Release 12.3(8)T and that is configured with a control plane with a class map to drop matched packets.

  Workaround: There is no workaround.

- CSCin82862

  Symptoms: Multicast traffic is not switched from a multilink interface on a Cisco 7500 series that is configured for distributed multilink PPP (MLP).

  Conditions: This symptom is observed when the router is reloaded or when the multilink interface flaps.

  Workaround: Enter the **clear ip mds linecard *** command on the Route/Switch Processor (RSP).

- CSCin83445

  Symptoms: Incoming multicast traffic on a distributed MLP link is process-switched.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed MLP after the router has been reloaded.

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

- CSCin84542

  Symptoms: A VWIC multiflex trunk controller may not come up.

  Conditions: This symptom is observed when you boot a Cisco 3745 that runs Cisco IOS Release 12.3(7)T6. This problem will only occur with **alarm trigger-blue** command enabled

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected controller after the router has booted.

- CSCin85992

  Symptoms: An EzVPN tunnel fails to come up on a dialer interface.

  Conditions: This symptom is observed when both a crypto map and an EzVPN client configuration are applied on the dialer interface. The output of the **show crypto map** command shows that the same static or dynamic crypto map is applied multiple times on the cloned virtual-access interface.

  Workaround: There is no workaround.

- CSCin86954

  Symptoms: A spurious memory access is generated after you have entered the **show running-config** command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(13) when a range of PVCs is configured on an interface or subinterface.

Workaround: There is no workaround.

- CSCin87008

  Symptoms: A router that runs SSG may reload when SSG is configured as a RADIUS proxy and processes access requests from RADIUS clients.

  Conditions: This symptom is observed when SSG is configured as a RADIUS proxy with a session identifier as the IP address and when SSG processes multiple simultaneous requests from RADIUS clients, all of which are assigned the same IP address.

  Workaround: Ensure that different sessions receive different IP addresses or configure another attribute such as MSID to ensure that there is a unique attribute as the session identifier in an access request.

- CSCin87071

  Symptoms: A router that runs SSG may reload when SSG is configured as a RADIUS proxy and processes retransmitted access requests from RADIUS clients.

  Conditions: This symptom is observed when SSG is configured as a RADIUS proxy with a session identifier as the IP address and when SSG processes multiple simultaneous requests from RADIUS clients, all of which are assigned the same IP address and some of which are retransmitted.

  Workaround: Ensure that different sessions receive different IP addresses or configure another attribute such as MSID to ensure that there is a unique attribute as the session identifier in an access request.

- CSCin87258

  Symptoms: A Cisco router that is configured for SSG may reload when you configure a local service profile.

  Conditions: This symptom is observed when the local service profile is configured with more than 150 service network entries.

  Workaround: There is no workaround.

- CSCin87464

  Symptoms: A spurious memory access occurs on an SSG when you run a MIB get request for the SSG service binding entries.

  Conditions: This symptom is observed when an SSG service is bound to a next-hop IP address.

  Workaround: There is no workaround.

- CSCin87560

  Symptoms: The following error message is displayed on a router that is configured for SSG:

  ```
  %SYS-3-BADLIST_DESTROY: Removed a non-empty list
  ```

  Conditions: This symptom is observed while you unconfigure an SSG feature by entering the **no ssg enable force-cleanup** command on the router that has one or more instances of an SSG service binding configuration such as the **ssg bind service** command (with the proper arguments that indicate a service name, IP address, interface type, and interface).

  Workaround: Before you unconfigure the SSG feature, unbind the SSG service by entering the **no ssg bind service** command (with the proper arguments that indicate a service name, IP address, interface type, and interface).

- CSCin87776

  Symptoms: Multilink bundles on a Cisco 7500 series may process-switch traffic instead of using dCEF, causing the CPU usage of the RSP to increase sharply and a CPU hog condition to occur.

  Conditions: This symptom is observed when an RPR+ switchover occurs on a Cisco 7500 series that is configured for HA.(The switchover causes an MLP to flap.) However, the symptom may also occur on a Cisco 7500 series that has a single RP (so, without a switchover) when an MLP link flaps.

  Workaround: There is no workaround. Note that the symptom does not occur when SSO is configured because the MLP state is maintained.

- CSCin88303

  Symptoms: The line protocol of unchannelized interfaces on a PA-MC-2T3+ port adaptor remains down although the link is up.

  Conditions: This is observed when you change from the channelized mode to the unchannelized mode by entering the **no channelized** command on the T3 controller of the PA-MC-2T3+ port adaptor.

  Workaround: There is no workaround.

- CSCin89146

  Symptoms: The G.728 codec calls fail on a SIP call leg of an IPIPGW.

  Conditions: This symptom is observed when the G.728 codec is configured on the SIP leg and when a “ptime” translation error occurs.

  Workaround: There is no workaround.

- CSCin89165

  Symptoms: SSG does not create host objects in RADIUS proxy mode.

  Conditions: This symptom is observed when SSG is configured in SSG proxy mode with the session identifier as IP.

  Workaround: Use other parameters apart from IP as the session identifier. If this is not a practical option, there is no workaround.

- CSCsa44716

  Symptoms: A router that is configured for URL filter may unexpectedly reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that has the Cisco IOS Firewall feature enabled.

  Workaround: There is no workaround.

- CSCsa46455

  Symptoms: A Cisco gateway that runs a TCL IVR voice application may reload when the voice application is unconfigured or reloaded.

  Conditions: This symptom is observed only when the voice application is unconfigured or reloaded while calls are still active for the voice application.

  Workaround: Ensure there are no calls active for the voice application before you unconfigure or reload it.

- CSCsa47020

  Symptoms: When Multilink Frame Relay (FRF.16) is configured on two bundled serial links and when the traffic rate is above 2 Mbps, packet loss occurs.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7500 series when you send a 64-byte Ethernet frame. The symptom does not occur when the frame size is 512 bytes or more.

Workaround: There is no workaround.

- CSCsa51612

  Symptoms: A router that is configured with IPSec sessions reboots consistently at periodic intervals because of a bus error. The output of the **show version** command shows the following error message:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(12.8)T.

  Workaround: There is no workaround.

- CSCsa53062

  Symptoms: A DSP may hang when a SIP call uses DNS. The output of the **show voice call summary** command shows the following message:

  ```
  S_WAIT_HOST_DISC S_TSP_WAIT_RELEASE
  ```

  Conditions: This symptom is observed on a Cisco 1700 series that functions as a voice gateway and that is configured for DNS.

  Workaround: Disable DNS.

- CSCsa53127

  Symptoms: A bargeinable prompt aborts right after it starts playing, almost as if it is being barged in to.

  Conditions: This symptom is observed in the following scenario with an application that requests DTMF input using two to four digits with an asterisk as the termination character:

  - You let the prompt play (that is, you do not barge in).
  - You enter “123*”. The next prompt is a VXML Transfer element containing three .wav files (1.wav, 2.wav, and 3.wav).
  - This prompt is bargeinable, but you do not barge in. You hear a brief “burp”, but not the three .wav files.
  - The final prompt is non-bargeinable TTS “Test Passed”, which you hear just fine.

  Workaround: Make the .wav files non-bargeinable.

- CSCsa53685

  Symptoms: Incorrect VC12 defect information may be generated on a Cisco 7500 series that is configured with a PA-MC-STM-1.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S1.

  Workaround: There is no workaround.

- CSCsa53698

  Symptoms: Fax pass-through may fail.

  Conditions: This symptom is observed on a gateway that is configured for fax pass-through or T.38 with fax pass-through as the fallback method after an initial call is established, the gateway detects a fax tone, and the gateway sends a re-Invite message with a new SDP message requesting to switch to fax pass-through. However, the “o” line in the new SDP message has the same version ID as the

"o" line in the initial SDP request that was sent by the gateway. If the originating gateway does not indicate that it disabled silence suppression with a "silenceSuppression=off" attribute in its SDP answer, fax pass-through fails.

Workaround: There is no workaround.

- CSCsa54117

  Symptoms: A Cisco IAD2430 may become unresponsive to Telnet session and drop SIP registration because of a memory leak in the "CCSIP_SPI_CONTRO" process.

  Conditions: This symptom is observed on a Cisco IAD2430 that runs Cisco IOS Release 12.3(11)T2.

  Workaround: There is no workaround.

- CSCsa54608

  The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

  Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

  Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

  Only devices running certain versions of Cisco IOS are affected.

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

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

- CSCsa55048

  Symptoms: The content of the CEF table may be incorrect, causing less than optimal traffic conditions.

  Conditions: This symptom is observed when a static route is configured in one VRF and exported with an export map into another VRF and when this static route is added on two separate PE routers.

  Workaround: Do not configure the static router on both PE routers. If this is not an option, there is no workaround.

- 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.

- CSCsa58622

  Symptoms: When you enter the **show telephony-service all** or **show telephony-service** command and when the locale is set to Japan, a spurious memory access is caused by the command, and the following error message and traceback are generated:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x80EA5400 reading 0x2D0 %
ALIGN-3-TRACE: -Traceback= 80EA5400 80EA3938 803C3090 803C58EC 80ECC3D4
80EE851C 809098F8 8090CD1C %ALIGN-3-TRACE: -Traceback= 80EA56C4 80EA3938
803C3090 803C58EC 80ECC3D4 80EE851C 809098F8 8090CD1C
```

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release is 12.3(11)T, when Cisco CallManager Express is enabled, and when the **user-locale JP** or **network-locale JP** command is configured.

Workaround: There is no workaround.

- CSCsa59690

  Symptoms: A router reloads when you enter the **hardware-address** command.

  Conditions: This symptom is observed on a Cisco router that is configured for Dynamic Host Configuration Protocol (DHCP).

  Workaround: Edit the startup configuration to eliminate the configuration of the **hardware-address** command and reload the router with the modified startup configuration.

- CSCsa61378

  Symptoms: A Cisco router that is configured for SSG may hang or crash.

  Conditions: This symptom is observed when upstream traffic is sent immediately after a host logs in and the system is busy.

  Workaround: There is no workaround.

- CSCsa61864

  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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa64885

  Symptoms: A router that is configured for SSG intermittently resets itself and generates a spurious memory access.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T with a prepaid or proxy service that has an idle or session timeout configured in the service profile.

  Workaround: There is no workaround.

- CSCsa65656

  Symptoms: SSG uses a duplicate Acct-session-id (attribute 44) in a RADIUS accounting packet.

  Conditions: This symptom is observed for post-paid users.

  Workaround: There is no workaround.

- CSCsa66702

  Symptoms: A Cisco 3660 may reload when an IP phone is placed on hold.

  Conditions: This symptom is observed on a Cisco 3660 that runs Cisco IOS Release 12.3(11)T4.

  Workaround: There is no workaround.

- CSCsa71596

  Symptoms: The prompt file that is stored on an HTTP file server and that is invoked by a VXML document is not heard by a caller.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS interim Release 12.3(12.12)T5 when a VXML document attempts to retrieve and render a wav file that is stored on an HTTP file server.

  Workaround: There is no workaround.

- CSCuk52814

  Symptoms: A Cisco AS5400 does not complete a circuit-switched 64k-bit/s ISDN unrestricted data call over a VoIP dial peer. The call fails with release cause code 44 (requested circuit/channel unavailable).

  Conditions: This symptom is observed on a Cisco AS5400 that runs Cisco IOS Release 12.2 or Release 12.3(3g).

  Workaround: There is no workaround.

- CSCuk56024

  Symptoms: 6PE traffic is dropped on a PE router.

  Conditions: This symptom is observed when an IPv6 prefix is first learned by an OSPF IGP on a 6PE router but then no longer received by OSPF but iBGP on the 6PE router. The label information is properly updated in the RIB but not in the FIB.

  Workaround: Clear the route to restore proper forwarding.

- CSCuk56028

  Symptoms: Redistributed BGP IPv6 unicast routes are not advertised to any BGP peer even though they are shown as the best path. The output of the **show bgp ipv6 unicast** *ipv6-prefix* command shows that the best path route is “Not advertised to any peer.”

  Conditions: This symptom is observed when BGP IPv6 is configured to redistribute a better (that is, numerically lower) distance route, for example, when the **redistribute ospf** address family configuration command is enabled with an administrative distance of 110.

  The symptom normally occurs only for originating iBGP routes (for example, with an administrative distance of 200) because redistributing eBGP routes have a lower distance (for example, an administrative distance of 20).

  Workaround: There is no workaround.

- CSCuk56412

  Symptoms: An ATM interface of a PA-A3 ATM port adaptor may stop transmitting traffic, the output of the **show interface atm** *slot/port* command may show that output drops increment, and the connectivity may stop entirely.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.3(12.7).

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

  Alternate Workaround: Enter the **clear interface atm** *slot/port* command on the affected interface.

TCP/IP Host-Mode Services

- CSCsa62111

  Symptoms: A Cisco 7200 series router may see packets stuck in the input queue.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.3(12.10) with an NPE-G1.

  Workaround: Reloading the router will clear the input queue, or increasing the input queue using the **hold-queue** *length* command beyond the default limit of 75.

Wide-Area Networking

- CSCea30197

  Symptoms: When the *keep-exchanges* argument in the **frame-relay lmi-n391dte** *keep-exchanges* command has a value that is lower than 3, Frame Relay Autosensing does not function.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series but may be platform-independent.

  Workaround: Ensure that the value of the *keep-exchanges* argument is not lower than 3.

- CSCef58201

  Symptoms: The CEF-Dialer feature fails to add an adjacency for a virtual-access1 CEF interface because the IP route is installed after the feature attempts to add the adjacency.

  Conditions: This symptom is observed during a test on a Cisco router that runs Cisco IOS Release 12.3 or interim Release 12.3(10.3)T.

  Workaround: Configure a static host entry for the neighbor in the routing table, pointing to the Dialer interface:

  ip route *prefix mask* **255.255.255.255 Dialer1**

  For the *prefix mask* argument, enter the IP address of the neighbor.

- CSCeg16752

  Symptoms: A router may report a memory leak in the X.25 background process. When the router runs out of memory, it crashes with a watchdog timeout error.

  Conditions: This symptom is observed on a Cisco 3600 series that runs Cisco IOS Release 12.2(23) or Release 12.2(26).

  Temporary Workaround: Reload the router before the available memory becomes too low.

- CSCeg43033

  Symptoms: A Cisco 7200 series periodically shows incorrect adjacencies for the loopback address. The output of the **show ip cef events** *ip-prefix* command shows the following:

  ```
  <ip-prefix>/32, version 8177, epoch 0, attached, connected 0 packets, 0 bytes tag
  information set local tag: implicit-null via Loopback0, 0 dependencies valid discard
  adjacency
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(9b) and that is configured for PPP and CEF. However, the symptom maybe platform-independent.

  Workaround: There is no workaround.

- CSCeg61278

  Symptoms: A router that is configured for ISDN may reload because of a SegV exception.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(12) only when the BRI-NET3 switch type is configured and when the BRI interface emulates the network side. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeg67829

  Symptoms: A Cisco 7500 series may crash when you enter the **microcode reload** command.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dLFIoATM, dLFIoFR, and dLFI over leased line and that has the **scheduler heapcheck process memory processor** command enabled.

  Workaround: There is no workaround.

- CSCeg87685

  Symptoms: A Cisco gateway with a BRI interface may fail to include a bearer cap in the outgoing setup message for a SIGO call. This situation causes a QSIG supplementary services call to fail.

  Conditions: This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.3(8)T6 or interim Release 12.3(11)T2. The symptom does not occur in Release 12.3.

  Workaround: There is no workaround.

- CSCeg90765

  Symptoms: Data traffic that is received on a Multilink PPP over ATM (MLPoA) connection may be dropped.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for MLPoA and CEF switching.

  Workaround: Disable CEF switching.

- CSCeh32353

  Symptoms: A LNS intermittently routes packets to an incorrect interface in the process-switching path, preventing some applications from working properly. These applications such as ARP, CBAC, and NAT depend on the first packet to go to process-switching for their initialization operation. Consequently, this situation may affect user connectivity to the Internet.

  Conditions: This symptom is observed when the next-hop ISP router is connected via static routes and when there is no ARP entry on the LNS.

  Workaround: There is no workaround.

- CSCeh41079

  Symptoms: Packets get CEF switched even though the interface is configured for dCEF.

Conditions: This symptom is observed on a Cisco 7500 series router when the dialer legacy/profile is configured.

Workaround: There is no workaround.

- CSCsa44139

  Symptoms: When CMNS is configured with an X.25 hunt group, the CMNS connection may not be established over an Ethernet interface. This situation affects proper loadbalancing and redundancy.

  Conditions: This symptom is observed when the parallel serial interface in the X.25 hunt group is down and when the CMNS connection over the Ethernet interface is not yet established when the serial interface goes down.

  Workaround: Do not use an X.25 hunt group. Rather, use alternative X.25 addressing.

  Alternate Workaround: Enter the **clear x25 serial** *number* **ethernet** *number mac-address* command. Doing so enables you to activate the CMNS connection.

- CSCsa48125

  Symptoms: Outgoing calls fail on ISDN Non-Facility Associated Signaling (NFAS) group members that do not have a D-channel.

  Conditions: The symptom is observed when outgoing calls are made via NFAS group members that have the **nfas_d none** keyword configured.

  Workaround: There is no workaround.

- CSCsa52807

  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.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCsa56443

  Symptoms: IPCP does not come up because it does not negotiate.

  Conditions: This symptom is observed on a Cisco platform when certain AAA peruser attributes are downloaded from a RADIUS server. One example is an absolute timeout or idle timeout without any other peruser attributes; such as configuration causes PPP to stall before starting IPCP.

  Workaround: Configure values on the platform rather than downloading them from the RADIUS server.

- CSCsa71228

  Symptoms: When the **dialer map** command is configured on the dialer interface for rotary group kind of configuration, callback does not take place.

  Conditions: The **dialer map** command must be configured on the dialer interface.

  Workaround: Configure the **dialer string** command in the dialer profile configuration.

- CSCsa78148

  Symptoms: A Cisco router that functions as an L2TP Network Server (LNS) may drop sessions when multilink is enabled and negotiated on a forwarded inbound VPDN session.

  Conditions: This symptom is observed when LCP renegotiation of proxy negotiations is disabled (which is the default) and when the multilink Endpoint Discriminator option that is advertised by the LAC does not match the Endpoint Discriminator on the LNS.

  Workaround: Enable the LNS to renegotiate LCP when necessary by entering the **lcp renegotiation on-mismatch** VPDN group configuration command.

  Alternate Workaround: Avoid the need to renegotiate by entering the **ppp chap hostname** or **ppp multilink endpoint** command to configure matching Endpoint Discriminators on the LAC and LNS.

  Warning: Technically, the current behavior of the Cisco IOS software is correct. An LNS should not accept the results of a LAC proxy negotiation when the LAC negotiates values that do not accurately represent the LNS. A platform must be configured to either enable the LNS to renegotiate when necessary, or (if it is desired to avoid such renegotiations, which may be necessary to get around problematic client implementations) enable the LAC to negotiate adequately as a substitute for the LNS.

  The fix for CSCsa78148 deliberately introduces the behavior that a mismatched multilink Endpoint Discriminator is ignored when the LNS is configured to terminate connections on mismatched conditions. This behavior is introduced to prevent the termination of a connection for a condition that is harmless for the majority of VPDN users. From a technical standpoint, this behavior is improper because it means that the VPDN clients have an invalid notion of the identity of the peer. This situation may pose problems for clients who have more than one multilink-capable link active at a time because the invalid Endpoint Discriminators may prevent links from being properly bundled at the client end. In such circumstances, enabling LCP renegotiation or ensuring that the LAC and LNS agree on negotiation parameters is the only valid option.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Copyright © 2005–2012 Cisco Systems, Inc.
All rights reserved.