

Caveats for 12.4(2)T through 12.4(9)T2

- [Resolved Caveats—Cisco IOS Release 12.4\(9\)T2, page 1126](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(9\)T1, page 1143](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(9\)T, page 1163](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T11, page 1181](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T10, page 1183](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T9, page 1188](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T8, page 1192](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T7, page 1202](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T6, page 1214](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T5, page 1223](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T4, page 1223](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T3, page 1236](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T2, page 1249](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T1, page 1250](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(6\)T, page 1268](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T8, page 1271](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T7, page 1285](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T6, page 1287](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T5, page 1289](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T4, page 1296](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T3, page 1306](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T2, page 1320](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T1, page 1338](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(4\)T, page 1343](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T6, page 1354](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T5, page 1371](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T4, page 1385](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T3, page 1396](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T2, page 1405](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T1, page 1418](#)
- [Resolved Caveats—Cisco IOS Release 12.4\(2\)T, page 1427](#)
- [Obtaining Documentation and Submitting a Service Request, page 1437](#)

Resolved Caveats—Cisco IOS Release 12.4(9)T2

Cisco IOS Release 12.4(9)T2 is a rebuild release for Cisco IOS Release 12.4(9)T. The caveats in this section are resolved in Cisco IOS Release 12.4(9)T2 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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.

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.

IP Routing Protocols

- 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.

- 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.

- CSCek42700

Symptoms: A network and host-based configuration download over serial HDLC with an IP address obtained via SLARP fails.

Conditions: This symptom has been observed with a router that has no startup- configuration (after using the **write erase** command) but is staged for autoinstall over a serial link. An IP address is obtained, but the download fails with the following error message:

```
%Error opening tftp://255.255.255.255/network-config (Socket error)
```

```
%Error opening tftp://255.255.255.255/cisconet.cfg (Socket error)
```

Without this feature, router deployment with automatic configuration download at remote sites over serial interface is not possible.

Workaround: Use another method of autoinstall if possible, or pre- configure the router before deployment.

- 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 symptom 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.

- CSCse68877

Symptoms: A label mismatch may occur between the CEF table and the BGP table, and a new label may not be installed into the CEF table.

Conditions: This symptom is observed after a BGP flap has occurred on a Cisco router that is configured or MPLS VPN but that does not function in an inter-autonomous system and that does not have multiple VRFs.

Workaround: There is no workaround. After the symptom has occurred, enter the **clear ip route** command for the affected VRF.

- CSCse81684

Symptoms: A router running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:

```
---- Partial decode of process block ----
Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540
```

Conditions: This is seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

Workaround: Prevent the router from receiving a fragmented skinny packet by ensuring the path MTU between the call manager server and the router is large enough. Usually skinny packets aren't larger than 800 bytes.

- 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).

- CSCsf11052

Symptoms: Error messages are seen such as the following example:

```
%NHRP-3-PAKREPLY: Receive Resolution Reply packet with error - insufficient
resources(5) and data packets that should be taking a direct spoke-spoke tunnel are
taking the spoke-hub-spoke path.
```

Conditions: This symptom has been observed in a DMVPN Phase 3 Network when building or refreshing a spoke-spoke tunnel.

Workaround: See the Further Problem Description for how to manually see and clear the problem. The fix for CSCsd74859 "DMVPN Phase 3: Network NHRP mappings are not refreshed when being used" will help reduce the occurrence.

Further Problem Description: Use the **show ip nhrp** command to look for NHRP mapping entries that are covered by an NHRP network mapping entry in the table.

Example:

Network mapping:

```
192.168.13.0/24 via 10.0.0.13, Tunnel0 created 00:02:51, expire 00:07:08
  Type: dynamic, Flags: router nat
  NBMA address: 172.16.3.1
```

Incomplete mapping covered by above network mapping

```
192.168.13.70/32, Tunnel0 created 00:02:51, expire 00:00:13
  Type: incomplete, Flags: negative
  Cache hits: 61
```

```
192.168.13.72/32, Tunnel0 created 00:02:51, expire 00:00:13
  Type: incomplete, Flags: negative
  Cache hits: 16
```

If this example indicates the symptom is present. Clearing the incomplete mappings clears the symptom, but it can easily come back.

Example:

clear ip nhrp 192.168.13.70

- CSCsf11980

Symptoms: On Cisco IOS interim Release 12.4(9.16)T when running a DMVPN configuration with dual hub routers and with OSPF as the IGP, the router may experience a crash as NHRP attempts to send a NHRP resolution request.

Conditions: This symptom has been observed on routers with Cisco IOS interim Release 12.4(9.16)T when running a DMVPN configuration with dual hub routers and with OSPF as the IGP.

Workaround: There is no workaround.

- CSCsg22426

Symptoms: A router running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:

```
---- Partial decode of process block ----
Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540
```

Conditions: This is seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

Workaround: Prevent the router from receiving a fragmented skinny packet by ensuring the path MTU between the call manager server and the router is large enough. Usually skinny packets aren't larger than 800 bytes.

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

- 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

- 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.

- CSCek39470

Symptoms: A Cisco IOS router running Cisco IOS Release 12.4 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.

Conditions: 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) that is being used in a router with the **crypto ipsec** command configured.

- CSCek45222

Symptoms: No QoS service policy can be applied to the VLAN interface.

Conditions: This symptom has been observed when the **service- policy** command was blocked for all VLAN interfaces under all conditions.

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.

- CSCek46189

Symptoms: Forced target probing functionality in OER is affected.

Conditions: This symptom has been observed when the policy changes and only following a particular scenario in which learned prefixes are deleted and new policies take into effect.

Workaround: There is no workaround.

- CSCek49375

Symptoms: A Cisco GGSN running Cisco GGSN Release R5.2 may reload with a bus error while creating a PDP.

Conditions: This symptom has been observed in the following conditions.

1. A GTPv0 service-aware PDP from SGSN S1 on a transparent-mode APN is created.
2. The same create request comes from SGSN S2 on the existing PDP.
3. The PDP is deleted.
4. Now before the path is deleted, another GTPv0 service-aware PDP created from SGSN S1 is received.

Workaround: Use a non-transparent mode APN.

- 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.

- 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.

- CSCin99850

Symptoms: A Cisco GGSN crashes while executing the **show gprs gtp pdp tid tid** command under condition of multiple PDP creates and deletes.

Conditions: This symptom has been observed when multiple PDPs are created and deleted.

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.

- 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.

- CSCsd50476

Symptoms: The serial link goes down.

Condition: When T1/E1 controller is configured with channel-group, the Serial link goes down so the cem interface would not come up.

Workaround: There is no workaround.

- CSCsd71911

Symptoms: Application code accessing an already free'd block caused the malloc failures on Cisco 7200 router.

Conditions: This symptom has been observed when QoS malloc failure on a Cisco 7200 router occurs.

Workaround: There is no workaround.

- CSCsd76596

Symptoms: In Cisco Gateway GPRS Support Node (GGSN) running Cisco GGSN Release 5.2 or Release 6.0 software, all categories of the service-aware PDP might go into IDLE state upon receiving a duplicate PDP create request.

Conditions: This symptom has been observed when a Cisco GGSN gets a duplicate Create PDP request for the existing service-aware PDP.

Workaround: There is no workaround.

- CSCsd81183

Symptoms: Mallocfail error messages and tracebacks are seen on the Cisco 1802W router due to normal particle pool memory leaks.

Conditions: This symptom has been seen on a Cisco 1802W router that is running Cisco IOS Release 12.4(6)T with the command "qos pre-classify" enabled under the virtual tunnel interface.

Workaround: Disable the HW encryption, or disable "qos pre-classify".

- 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.

- 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>

- 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.

- CSCse50167

Symptoms: Speed dial line buttons disappear from CME phones after a router reload.

Conditions: This symptom has been observed when the speed dial buttons are configured under an ephone template which is applied to the affected phone. The CME is reloaded.

Workaround: Remove and reapply the ephone template through the ephone commands after the router reloads.

- 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.

- 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.

- CSCse56800

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>.

- 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

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

- CSCse69102

Symptoms: Spurious memory access made at ike_profile_remove

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS 12.4(6)T3, when there is at least one ike or ipsec sa and the profile is removed using the CLI with debug crypto isakmp turned on.

Workaround: Turn off crypto isakmp debugs or clear all the crypto sessions and then remove the isakmp profile.

- 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.

- CSCse80519

Symptoms: The router may reload when it receives XML.

Conditions: This symptom has been observed when Cisco IOS had been configured to receive XML. A line similar to <lica:request xmlns:lica="http://www.website.com/LA"> is in the XML. That is a XML namespace is being declared.

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

Symptoms: 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 12.4Mainline and 12.4T release

Workaround: There is no workaround.

- 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.

- 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.

- CSCse93695

Symptoms: Three-way calls that involve a third-party vendor SIP server and Cisco IAD2400 series Integrated Access Devices may not work.

Conditions: This symptom 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.

- CSCsf03412

Symptoms: Using 'boot flash' or boot tftp crashes router.

Conditions: This symptom has been observed with Cisco IOS interim Release 12.4(7.24)T on a Cisco 3845 router.

Workaround: There are three possible workarounds:

Method 1: If using an older image, i.e. 12.3(11)T, is acceptable, use it.

Method 2: If necessary to use 'boot flash', use 'boot flash:' instead.

Method 3: If necessary to use "boot tftp", copy the image to flash and use "boot flash:".

- 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.

- CSCsf05693

Symptoms: A router may unexpectedly reload after reporting "Unexpected timer" errors similar to:

```
Aug 6 17:29:16.908 GMT: %SIP-3-BADPAIR: Unexpected timer 19
(SIP_TIMER_NOTIFY_RECEIVE_DIGIT) in state 10 (STATE_DEAD) substate 0 (SUBSTATE_NONE)
```

Conditions: The router must be configured for SIP.

Workaround: There is no workaround.

- CSCsf09266

Symptoms: EasyVPN negotiation fails when using EasyVPN with VTI. A %CRYPTO-6-IKMP_MODE_FAILURE will be printed to the console.

Conditions: This symptom has been observed when using EasyVPN with VTI.

Workaround: Remove VTI from the EasyVPN configuration.

- 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.

- CSCsf11855

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>

- CSCsf19418

Symptoms: Entering the Command Line Interface command **show mpls ldp graceful-restart** may lead to a router restart.

Conditions: The router will restart if the command output has a Down Neighbor Database entry that entry expires by reaching the reconnect timeout limit when output is printing the neighbor Address list. The router will also restart upon continuing the Command Line Interface output page if the string “--More--” within the context of displaying addresses.

Workaround: Avoid entering **show mpls ldp graceful-restart** when a graceful-restart database entry is about to expire. If console output is paged at “--More--” entry in the address list context, and the Down Neighbor Database entry may have expired, type the letter “Q” to abort any more output of addresses.

- 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.

- 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.

- 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 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.

- 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.

- CSCsg15837

Symptoms: WCCP service redirection does not work.

Conditions: WCCP redirection is configured on a router where the traffic being redirected enters an interface in a security zone.

Workaround: Remove zone assignment from requests's ingress interface.

- CSCsg15896

Symptoms: A Cisco AS5400XM gateway sees a lot of DSM errors:

```
%DSM-3-INTERNAL: Internal Error : No DSM handle provided
along with a traceback
```

Conditions: Occurs if using as Cisco AS5xxxXM gateway with the AS-5x-FC DSPs and an NFAS PRI and trying to configure (or unconfigure) input gain or output attenuation under the voice-port for the NFAS PRI with the latest 12.4T interim IOS.

Workaround: There is no workaround.

Further Problem Description: If using Cisco IOS Release 12.4.9T1 or earlier, the symptom causes an unexpected reload of the Cisco AS5xxxXM gateway with a bus error.

- 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>.

- CSCsg22426

A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

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

- CSCsd74139

Symptoms: HTTP errors occur while accessing a Win2003 Web Server.

Conditions: This symptom has been observed with a Cisco IOS Voice gateway running Cisco IOS Release 12.4(6)T accessing a Win2003 HTTP web server under heavy load. Cisco IOS Voice has **ip http client connection persistent** disabled.

Workaround: There are two possible workarounds:

1. Switch to a Win2000 HTTP web server.
2. On a Win2003 server, set "TcpTimedWaitDelay" to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

- CSCsg26634

Symptoms: CPUHOG can occur when running lots of BGP connections.

Conditions: This symptom has been observed with RPM images during Service Provider testing of BGP running Cisco IOS Release 12.4(6)T.

Workaround: There is no workaround, though the symptom was quickly found and repaired.

Wide-Area Networking

- CSCek31887

Symptoms: Some supplementary services does not work because of QSIG rose_decode_facilityIE problem

Conditions: This symptom has been seen in Cisco IOS Release 12.4(5.13)XC because of memory leak DDTs committed.

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 12.3, 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.

- CSCek58406

Symptoms: Router crashes shortly after changing encapsulation from fr -> hdlc.

Conditions: IPS configured on a map and an interface. First remove IPS from the map and then from the interface. Change the encapsulation.

Workaround: Remove the interface IPHC configuration first.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCse80942

Symptoms: Layer2 will be in the down state for the basic-qsig switch type.

Conditions: This symptom has been observed for the basic-qsig switch type in Cisco 3700 routers.

- Workaround: Bring the BRI interface UP by changing the switch-type from basic- qsig to basic-net3.
- 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.
 - CSCsf96318

Symptoms: 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.
 - CSCsg25693

Symptoms: Layer2 of BRI interfaces is not coming up, and it is in the “NOT Activated” state.

Conditions: This issue is seen in Cisco IOS interim Release 12.4(11.1)T.

Workaround: There is no workaround.
 - CSCsg38412

Symptoms: When a PPP Multilink session is established over ISDN on a router running Cisco IOS version 12.2SB, IPCP fails to negotiate. When **debug ppp negotiation** is enabled, it shows that IPCP packets from the peer are not processed. The output of **show interface** 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 RADIUS is used to assign the multilink bundle to a VRF.

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

Resolved Caveats—Cisco IOS Release 12.4(9)T1

Cisco IOS Release 12.4(9)T1 is a rebuild release for Cisco IOS Release 12.4(9)T. The caveats in this section are resolved in Cisco IOS Release 12.4(9)T1 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCek32177

Symptoms: The TACACS+ AV addr=255.255.255.254 will not be processed correctly with Cisco IOS interim Release 12.4(5.8)T or later.

Conditions: The symptom has been seen in testing Tacacs+ while the same scenario works fine with Radius.

Workaround: There is no workaround.

- 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.

- 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 sent and when an AAA server is slow or unreachable.

Workaround: There is no workaround.

- 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.

- CSCsd90875

Symptoms: A Cisco 3745 router crashes with ipsla_rtp_cfg test after starting ip sla schedule with Cisco IOS Interim Release 12.4(7.18)T.

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

```
config terminal
controller T1 1/0
ds0-group 0 timeslots 1 type none
ds0-group 1 timeslots 2 type none
ds0-group 2 timeslots 3 type none
ip sla 1
voip rtp 10.10.10.1 source-voice 1/0:1 codec g711u
timeout 10000
exit
ip sla sch 1 star now life 300
```

Workaround: There is no workaround.

- 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.

- 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.

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.

- CSCek47475

Symptoms: bgp ipv4 session could not be up.

Conditions: This symptom occurs on Cisco IOS interim Release 12.4(9.15)T only.

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, 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.

- CSCse51804

This caveats consists of two symptoms, two conditions, and two workarounds:

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.

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.

- CSCse64256

Symptoms: When a First Hop Router receives (S,G) stream for an Embedded RP group, it might crash while trying to send register packets.

Conditions: This symptom has been observed when trying to send register packets.

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.

- 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

- 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.

- 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.

- CSCek42062

Symptoms: Router crashes consistently within minutes of making a call from a Cisco 7920 Wireless IP Phone registered to CME 4.0 via a wireless connection. The crash points to memory corruption.

Conditions: This symptom has been seen on Cisco IOS Release 12.4(4)XC.

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.

- 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.

- CSCek44071

Symptoms: Incoming SS7 calls with Loopback Continuity Testing (COT) fail to setup.

Conditions: This symptom occurs with basic 1 call bringup using Loopback COT.

Workaround: There is no workaround.

- CSCek44714

Symptoms: When using GDOI and the crypto engine is VAM2+, the crypto engine throws an invalid attribute error.

Conditions: This symptom has been observed when using VAM2+ with GDOI.

Workaround: Use software Crypto.

- 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.

- 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 Cisco IOS Release 12.4 and Release 12.4T.

Workaround: There is no workaround.

- CSCek47681

Symptoms: Under heavy stress, a few TDM backplane timeslots (3 or 4) are lost after 12 hours.

Conditions: This symptom has been seen with SS7 with more than 50 calls per second.

Workaround: There is no workaround.

- CSCek48151

Symptoms: When a forced target is used for active probing, then actual probing may not occurring certain conditions. OER looks for a route to a prefix created using the forced target and the mask length of the prefix to which the forced target is assigned. If the route doesn't exist or super route doesn't exist, then probes are not created. For example:

```
Prefix: 10.1.1.0/24
Forced Target: 10.2.2.2
Routes on BR:
10.2.2.2/32 via Exit1
10.1.1.0/24 via Exit1
```

Even though there is a route to 10.2.2.2, it will not be probed because OER looks for route 10.2.2.0/24 formed by the target IP 10.2.2.2 and mask length 24 of the prefix 10.1.1.0/24.

The symptom would not occur if there are default routes through all exits.

Conditions: This symptom has been observed when a forced target is used for active probing.

Workaround: Create a route to the prefix formed by the target IP and the mask length of the prefix to which it is assigned or create a default route.

- CSCek49023

Symptoms: The passive monitoring of applications using DSCP as part of application definition is not working because the conversion from DSCP to ToS is missing.

Conditions: This symptom has been observed with applications using DSCP.

Workaround: There is no workaround.

- CSCek50471

Symptoms: With a certain combination of debugs enabled, the packet contents are being displayed. This should be avoided with GDOI because there is sensitive information being displayed.

Conditions: This symptom has been observed with a certain combination of debugs enabled.

Workaround: There is no workaround.

- CSCsa43170

Symptoms: A Cisco 2600XM series router may unexpectedly restart while handling a bus error. The original bus error was going to result in an unexpected restart. However the data normally saved after such an event may not be completely saved due to the second unexpected restart.

Conditions: This symptom affects Cisco IOS software after Cisco IOS Interim Release 12.3(10.3)T2 only on the Cisco 2600XM series of routers.

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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsd04581

Symptoms: When EasyVPN is configured to use a BRI interface as the outside interface, return packets may fail to decrypt properly within the router.

Conditions: This symptom has been observed when EasyVPN is configured.

Workaround: Disable the onboard crypto accelerator.

- 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.

- CSCsd30632

Symptoms: OSPF and LDP periodically may go down on a Cisco MGX-RPM-XF-512 running Cisco IOS Release 12.3(11)YW1. The protocols may be down for 2 to 3 minutes and then self recover.

Conditions: This symptom has been observed on a Cisco MGX-RPM-XF-512 running Cisco IOS Release 12.3(11)YW1.

Workaround: There is no workaround.

Further Problem Description: Input queue may show Input queue: 776/600 Input OAM queue may show Input OAM Queue: 775

- 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.

- CSCsd35269

Symptoms: The router resets when switching ipv4 or ipv6 traffic over CEF from one tunnel to another.

Conditions: This symptom has been observed on a Cisco 7200 router with back-to-back tunnels and CEF switching.

Workaround: Do not configure the **ip cef** global configuration command or the **ipv6 cef** global configuration command.

- 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.

- CSCsd68767

Symptoms: This assertion indicates that the router has dropped an incoming packet due to a known bug in the FIO/GIO. A particle may have been leaked in I/O memory. This is expected to be an extremely rare occurrence; no action is necessary unless it happens repeatedly. Under certain (not well-understood) conditions, this bug may result in an unexpected system reload.

Conditions: This symptom has been observed with ADSL traffic flowing on ADSL port of HWIC_ADSL_BRI card, at high traffic volume, and on more than one PVC.

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.

- 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.

- 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.

- 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>

- 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.

- CSCse04136

Symptoms: A router crashes with traceback.

Conditions: This symptom has been observed when a Cisco 7200 router is sending traffic using IXIA after applying crypto map feature.

Workaround: There is no workaround.

Further Problem Description: The crash was obtained when testing TED feature in Cisco 7200 routers using IXIA. While sending packet to initiate IPSec tunnel, the router got crashed with traceback

- CSCse05292

Symptoms: Static map configuration for ATM PVC using **protocol ip IP address** command is rejected, giving error as ambiguous command.

Conditions: Configure static map on ATM PVC using **protocol ip IP address** command

Workaround: There is no workaround.

- CSCse06975

Symptoms: VoIP LMR multicast capability does not work on a network module NM-HD-2V with E&M.

Conditions: This symptom has been observed on a network module NM-HD-2V with E&M.

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 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
```

- 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.

- CSCse18940

Symptoms: Memory depletes over short time when VoAAL2 traffic is passed.

Conditions: PVDM2-64 module is used to pass VoAAL2 traffic.

Workaround: None

- CSCse24428

Symptoms: When the PMC PTT key is pressed on a channel shared by an LMR voice port configured for e-lead voice, the e-lead is not seized.

Conditions: This symptom occurs on Cisco IOS Release 12.4(6)T or Cisco IOS Release 12.4(4)T with versions of VIC2-2E/M hardware older than HW version 5.1.

Workaround: Use Cisco IOS Release 12.4(4)T with newer E+M hardware until issue is resolved.

- 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.

- CSCse40276

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>

- 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.

- CSCse44158

Symptoms: The radius account attribute feature-vsa attribute is being sent even though an accounting template has been applied commenting out the attribute.

Conditions: The symptom has been observed when the filter feature-vsa attribute is using the accounting template.

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.

- 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.

- CSCse53002

Symptoms: Memory leaks at IPSEC key engine process. In the show memory sum command, the memory block used as “KMI num ipsec” is leaking.

Conditions: This symptom has been seen if there is traffic.

Workaround: It may be possible to disable the hardware encryption. If not, 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_elt1_vic_connect: setup failed
Jun 20 01:41:15.855: flex_dsprmtdm_xconn: voice-port(0/0/1), dsp_channel
(/0/2/0)
```

Workaround: Disable caller id on the voice-port.

- CSCse58234

Symptoms: A router is crashing due to bad chunk reference count.

Conditions: This symptom occurs on Cisco 7200 routers running Cisco IOS Release 12.4(6)T2 configured for H.323 voice services.

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>

- CSCse75492

Symptoms: There is a possibility router crash due to fixing memory leak problem in “SSS Manager.”

Conditions: This symptom may happen in an LAC router.

Workaround: There is no workaround.

- CSCse83674

Symptoms: Analog FXS port on a Cisco 2800/3800 ISR does not go back to idle if it has been offhook for more than a minute at the end of a call.

Conditions: A and B are two FXS ports on the same router connected to analog phones. A calls B. B answers the call. Once the conversation is done, A hangs up. B does not go onhook. After 60 seconds, B starts hearing offhook alert (howler) tone. Putting B onhook now has no effect. B continues to play offhook alert for the rest of its life until the router is reloaded.

Workaround: There is no workaround.

- CSCse89402

Symptoms: The CPU stack frame can become corrupted when a channel-group is configured on the t1/e1 controller.

Conditions: This symptom have been seen on mainboard WIC slots when the slot is configured with the **no network-clock participate** command.

Workaround: Use the **network-clock participate** command to configure the VWIC 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.

- 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.

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.

- 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.

- 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.

- CSCse41463

Symptoms: A router which when configured with the **frame-relay ip rtp header- compression** command crashes with the traceback.

Conditions: This symptom is observed on Cisco 2600, Cisco 3745, and Cisco 7200 routers that run Cisco IOS Interim Release 12.4 (9.9)T.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(9)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(9)T. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(9)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- 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>

- 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.

- CSCek29332

Symptoms: The **ip sla monitor** command of type **voip** is rejected.

Conditions: This symptom has been observed with Cisco IOS interim Release 12.4(5.13)T2.

Workaround: Use the newer command versions of the **ip sla** command.

- 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.

- CSCsd49133

Symptoms: Alarms are not populated in the ceAlarmTable. The ceAlarmlist is empty. The whole entity alarm filtering functionality fails.

Conditions: When the connected interface at the peer device is shut, alarms should be populated in the ceAlarmTable -> ceAlarmList object. It can also be viewed using the CLI **show facility-alarm** status EXEC command. There are no issues observed in CLI. The **show facility- alarm** status EXEC command CLI shows alarms correctly. Only the ceAlarmTable -> ceAlarmList object is not getting populated.

Workaround: There is no workaround.

- CSCse09204

Symptoms: When upgrading from Cisco IOS Release 12.4(2)T or Cisco IOS Release 12.4(4)T, the IP SLAs echo operation configuration is lost. This defect is logged because the router (while coming up after reload) does not understand the use of "Dialer" in the *interface-name* argument of the **source-interface interface-name** command as shown in this example:

```
DRAM configuration is 64 bits wide with parity enabled.
```

```
239K bytes of non-volatile configuration memory.
```

```
250368K bytes of ATA CompactFlash (Read/Write)
```

```
type echo protocol ipIcmpEcho 10.0.0.1 source-interface Dialer1
```

```
% Invalid input detected at '^' marker.
```

```
timeout 1000
```

```
^
```



```
% Invalid input detected at '^' marker.
```

```
frequency 3
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
%Entry not configured
```

This symptom is related to CSCsc24145.

Conditions: This symptom has been observed on routers having the IP SLA echo operation configured with the **ip sla monitor** command, when these operations specify the Dialer as the source-interface, and when the router is being upgraded to Cisco IOS Release 12.4(4)T or later version.

Workaround: Reconfigure new operations with the new release after upgrading.

- CSCsg00102

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

IP Routing Protocols

- CSCej70091

Symptoms: Sending a ping to the router interface does not get an answer and results in traceback.

Conditions: This symptom has been observed when FPM service policy is configured on the interface.

Workaround: There is no workaround.

- CSCek16041

Symptoms: A Cisco 870 router does not offer the *vrf* keyword during configuration of the **router ospf** command:

```
router(config)#router ospf ? <1-65535> Process ID
```

```
router(config)#
```

Conditions: The symptom has been observed in Cisco IOS Interim Release 12.4 (5.8)T. Only the Cisco IOS Release 12.4T train is affected. The symptom is triggered by port of CSCsb73882 in Cisco IOS Release 12.4T.

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.

- CSCsc70155

Symptoms: A Telnet session from a TCP host to an X.25 client may fail when the protocol translator is configured in between.

Conditions: This symptom has been observed in Cisco IOS interim Release 12.4 (5.8)T.

Workaround: There is no workaround.

- CSCsc75409

Symptoms: Toggle the **no ip cef** command followed by the **ip cef** command could cause a router CPUHOG.

Conditions: This symptom is especially vulnerable on a router that is configured with many VRFs (maybe more than 100 VRFs) and with an import/export routes to each other.

Workaround: There is no problem if the command sequence **no ip cef** command followed by the **ip cef** command is not executed. If this command sequence is executed, there should be no problem if less than 50 VRFs are configured. As the number of VRFs that are configured is increased, the CPU utilization will rise. 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.

Miscellaneous

- CSCed28266

Symptoms: A Cisco gateway may unexpectedly reload because of a software-forced crash when it builds a SIP ACK(nowledge) or BYE message.

Conditions: This symptom is observed when the gateway receives a SIP response that contains a Record-Route header and a Contact header and when the length of the Contact header exceeds 128*n, in which "n" is the number of URLs in the Record-route header.

Workaround: There is no workaround.

- 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.

- CSCej40305

Symptoms: The router will crash when the testing script is aborted and the script is re-run without clearing out the existing configuration.

Conditions: This crash has not been seen under normal operating conditions and requires a sequence of events in the code path that are not easily identified. The crash is reproducible.

Workaround: Enter a **clear crypto gdoi** command on the key server to clear up some existing data structures to prevent the crash.

- 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.

- CSCej89156

Symptoms: RPM-XFL card is continuously rebooting with Cisco IOS Release 12.4T.

Conditions: This symptom has been observed with a VC tunnel priority queue configured with VC SCR rate.

Workaround: There is no workaround.

- CSCek10347

Symptoms: The Key Server crashes with the testing script and ipsec-dgvpn.

Conditions: This crash has not been seen under normal operating conditions and requires a sequence of events in the code path that are not easily identified. The crash is reproducible.

Workaround: There is no workaround.

- CSCek15980

Symptoms: A Cisco router may not set its interface identifier to the ID provided in an IPv6CP exchange.

Conditions: This symptom has been observed when running Cisco IOS Release 12.4T.

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.

- CSCek23826

Symptoms: Executing the **debug rpm hwdiags POS 1** command doesn't display any output.

Conditions: Execute the **debug rpm hwdiags POS 1** command on a standby RPM-XF from user mode and the same on an active RPM-XF from privileged mode.

Workaround: There is no workaround.

- CSCek23920
Symptoms: The **show policy-map interface sw1.xx** command output is jumbled and information pertaining to a class is not fully displayed under the correct class.
Conditions: With service policy-map attached to PVC execute **show policy-map interface sw1.xx** command
Workaround: There is no workaround.
- CSCek24060
Symptoms: A spurious memory access traceback has been observed.
Conditions: This symptom has been observed when an XF card reloads or resets from PXM.
Workaround: There is no workaround.
- CSCek24516
Symptoms: Memory corruption has been observed.
Conditions: This symptom has been observed when resetting the Multilink interface.
Workaround: There is 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 AS5400XM 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.
- 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>
- CSCek26569
Symptoms: Cisco 878 and Cisco 2691 routers crash while pinging with the **ip inspect** command configurations.

Conditions: This symptom has been observed with Cisco IOS interim Release 12.4 (6.6)T. Configure the **ip inspect** command on an interface and ping the IP address on the interface.

Workaround: There is no workaround.

- CSCek26595

Symptoms: After configuring Multicast and applying the **crypto map** command, traffic can't go through from the second Ethernet interface to the same group. However, traffic goes through fine from the first Serial interface.

Conditions: The symptom has been observed in Cisco IOS interim Release 12.4(5.13)T2.

Workaround: There is no workaround.

- CSCek27100

There are two customers' escalated issues which are related to the DSL Firmware 3.01.

1. Customer complaining on noise margin issue on CPE against a third-party vendor DSLM
2. DSL 878 not training up correctly to SHDSL third-party vendor DSLAM

Both customer and internal DevTest/InterOP lab have verify these problems are fixed by the new 3.05 firmware.

- CSCek27307

Symptoms: When registering an EEM Tcl policy with the **event_register_resource** command extension, an error message that the keyword **policy** is not supported will appear.

Conditions: This symptom has been observed when an EEM Tcl policy with the **event_register_resource** command extension is registered.

Workaround: There is no workaround.

- CSCek27437

Symptoms: An SNMP request to delete a switch connection (setting cwaChanRowStatus to 6 [destroy]) deletes both the Swconn part and the PVC part.

Conditions: This symptom has been observed under normal conditions using SNMP to manage connections on RPM.

Workaround: There is no workaround.

- CSCek27743

Symptoms: Ping can't go through after applying a crypto map.

Conditions: This symptom has been observed with Cisco IOS interim Release 12.4 (6.6)T.

Workaround: There is no workaround.

- CSCek28936

Symptoms: In the IP-MPLS path, the basic MPLS IP to Tag switching for optimum path fails.

Conditions: This symptom has been observed when running Cisco IOS interim Release 12.4(5.13)T3 and interim Release 12.4(5.13)T4.

Workaround: There is no workaround.

- CSCek29605

Symptoms: SIP phones do not receive MWI even though a message is left for a SIP phone user.

Conditions: This symptom has been observed with SIP phones on CME and when CUE has voicemail.

Workaround: There is no workaround.

- CSCek30276

Symptoms: A ping fails with port adapters (PA) inserted into a C7200-I/O Jacket Card with reformation images.

Conditions: This symptom only happens with reformation images and not with classic images.

Workaround: Use a classic image or use the PA in any other slot other than ESCORT.

- 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.

- CSCek32162

Symptoms: The Dot11 Radio interface does not come up.

Conditions: This symptom has been observed when using the following procedure:

1. Boot up the router with no configuration. Use the **erase startup-config** command and reboot the router.
2. Use the **no shutdown** command on the dot11 interface.
3. Configure the **ssid** command.
4. Configure the **authentication** command.

Workaround: Configure the **ssid** command and **authentication** command before using the **no shutdown** command.

- CSCek32263

Symptoms: The Parallel eXpress Forwarding (PXF) on RPM-XF card reloads and generates a log and a crashinfo file.

Conditions: Bit errors in PXF IRAM can occur, though they are extremely rare. The Bit error in PXF Instruction RAM can cause other issues, like invalid register contents, which could result in other PXF exceptions causing the reload.

Workaround: There is no workaround. The PXF crash process will reload PXF IRAM. All layer 3 connectivity comes up automatically after the PXF reloads.

- 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.

- CSCek35105

Symptoms: When the policy-map class bandwidth is modified, it fails for the multilink interface.

Conditions: This symptom has been observed with the output of the policy map attached to multilink and when changing the bandwidth allocation for a class.

Workaround: Use the **shutdown** command and then the **no shutdown** command on the switch subinterface.

- 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>

- CSCek41147

Symptoms: RFC2833 is not working between Cisco CallManager Express (CME) and a Cisco AS5850 gateway in a SIP trunk service.

Conditions: This symptom has been observed on a Cisco 2800 Series Integrated Services Routers (ISR) running Cisco IOS Release 12.4(4)T2 configured for CME SIP trunking. The VoIP dial-peer has the **dtmf-relay rtp-nte** command configured.

Workaround: The only workaround is to have the Cisco AS5850 gateway configured for RFC2833 if that is possible in the network. As this change will effect live deployment, it may not be possible, in which there is no workaround.

Further Problem Description: CME is not offering RFC2833 DTMF relay capability when VoIP dial-peer has the RFC2833 DTMF relay configured.

- CSCin98470

Symptoms: The microcode reload generates a CPU Hog traceback.

Conditions: This symptom has been observed on an RPM-XF card with more than 2k policy maps.

Workaround: There is no workaround.

- CSCin98900

Symptoms: Hardware diagnostics for Fast Ethernet always fail.

Conditions: This symptom has been observed when running the hardware diagnostics for the Fast Ethernet back card after plugging the card in.

Workaround: There is no workaround.

- 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.

- 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>.

- 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>.

- 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.

- 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.

- 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.

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 occur only on a single voice port, there is another problem, not this caveat (CSCsc11833). 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: 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
```

- 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.

- CSCsc46528

Symptoms: ccmeEphoneActTable from CISCO-CCME-MIB provides inconsistent results.

Conditions: This symptom has been observed when a partial SNMP GET is issued on selected columns from ccmeEphoneActTable.

Workaround: Perform a complete SNMP GET instead of a few entries on ccmeEphoneActTable.

- CSCsc59881

Symptoms: Call forward busy to Unity gets the subscriber standard greeting instead of the busy greeting.

Condition: This symptom has been observed when Unity integrates with CME 3.4.

Workaround: There is no workaround.

- CSCsc69380

Symptoms: A router crash may occur if FPM policies are configured and the CISCO-CLASS-BASED-QOS-MIB.my MIB is queried.

Conditions: This symptom has been observed when FRM policies are configured on routers running Cisco IOS Release 12.4T.

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.

- 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.

- 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.

- CSCsc80305

Symptoms: The radio fails to function with constant assertion fail and message shows Atheros Chipset met fatal error.

Conditions: 1. With total 384Mb memory (128Mb on board and 256Mb external DIMM memory) in a Cisco 2801 or Cisco 1841 router. 2. Use the **no shut** command in radio interface mode and configure any one SSID.

Workaround: Replace 256Mb DIMM with 128Mb DIMM.

- CSCsc80668

Symptoms: The Cisco IOS has the capability to implement HSP feature but the MIB support is incomplete. HSRP-related MIBs have not been implemented in the Cisco 800 series platforms.

Conditions: This symptom has been observed on Cisco 800 series routers.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsc94149

Symptoms: Cisco 876 and Cisco 877 routers fail to synchronize with third-party vendor DSLAMs.

Condition 1. The DSL line of a Cisco 876 router with the **dsl operating-mode auto** command configured fails to synchronize with a third-party vendor DSLAM and line card SU ADSL 32I (TI chipset).

Condition 2. The DSL line of Cisco 876 and Cisco 877 routers with the **dsl operating-mode auto** command configured fails to synchronize in ADSL2/2+ Rate-Adaptive mode with another third-party vendor DSLAM at and below 2000m line loop length with maximum data rates configured as 512/512 Kbps upstream and downstream.

Workaround 1. There is no workaround.

Workaround 2. For 512/512 Kbps profile, if the line operating mode is set to itu-dmt, the line trains up fine in ADSL1 mode.

- 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.

- CSCsc97545

Symptoms: On a Dynamic IPsec VTI, when a packet is greater than twice the IP MTU (i.e., needing more than 2 fragments), the first fragment is transmitted but not the additional fragments.

From the **show ip traffic** command:

- The "Fragments" counter is incremented by two.
- The "Couldn't fragment" counter is incremented by one.

Conditions: This symptom has been observed when an IP packet needs more than two fragments on a router serving as an IPSec Gateway using Dynamic IPSec VTI. It is only seen when Cisco Express Forwarding (CEF) is turned on.

Workaround: There is no workaround.

- 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.

- CSCsd02098

Symptoms: There is no voice path and packets are not encrypted or decrypted.

Conditions: This symptom has been observed when a call is made as an SRTP call.

Workaround: There is no workaround.

- CSCsd08392

Symptoms: RP-sourced control packets are delayed causing protocol timeouts.

Conditions: This symptom has been observed with VC congestion, when SAR-based- cbwfq is enabled, and when the output service policy is attached to the VC.

Workaround: There is no workaround.

- CSCsd10115

Symptoms: The gateway reloads during call transfer scenarios.

Conditions: This affects calls on a SIP-SIP CME or an IPIP GW, which is doing consultative transfer.

Workaround: There is no workaround.

- CSCsd17124

Symptoms: The Cisco 1812J router could crash due to:

1. An Illegal Opcode exception.
2. An Address error
3. A SegV Exception

Conditions: The symptoms have been observed on Cisco 1812-J routers with Cisco IOS Release 12.4(4)T and 12.4(6)T and Rommon Release 12.3(8r)YH6.

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.

- 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.

- CSCsd20136

Symptoms: Bidirectional Forwarding Detection (BFD) support was added for the Cisco 7200 and Cisco 7301 platforms in Cisco IOS Release 12.4(4)T. Some interface level BFD commands are not configurable which may prevent the full BFD feature from working.

Conditions: This symptom is seen with all feature set images of Cisco 7301 and Cisco 7200 of Cisco IOS Release 12.4(4)T and Cisco IOS Release 12.4(4)T1 except Cisco 7200 with GGSN feature set images of same versions.

Workaround: There is no workaround.

- CSCsd30932

Symptoms: Issuing the **trust-point storage** command sometimes causes a crash.

Conditions: This symptom only occurs when an error occurs on a previous execution of this command. The second execution of the command results in a crash.

Workaround: If an error occurs when issuing this command, the trustpoint must be removed and re-created to avoid a crash.

- 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.

- 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>

- CSCsd44693

Symptoms: Router crashes when sending trap related to tunnel down if the remote peer ID is FQDN.

Conditions: This symptom has been observed with the tunnel down and remote peer with FQDN ID.

Workaround: Do not use FQDN as a remote peer ID.

- CSCsd53422

Symptoms: The Parallel Express Forwarding (PXF) external column memory (XCM) cannot be read without superuser privileges.

Conditions: This symptom has been observed with an RPM-XF Cisco router running Cisco IOS Release 12.4T and earlier.

Workaround: There is no workaround.

- CSCsd55168

Symptoms: Protocol Independent Multicast (PIM)sparse mode (SM) Multicast-VPN (MVPN) Core is not working.

Conditions: The symptom has been observed in IPFR LSNT with MGX-based RPM-XF PEs and RPM-XF Hub/P routers, which uses Parallel Express Forwarding (PXF) for forwarding.

Workaround: There is no workaround.

- 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>

- CSCsd69754

Symptoms: Traffic through an IPsec VPN connection does not leave the router.

Conditions: This symptom has been observed when the interface where the **crypto map** command is applied (the interface that will be the source address of the encrypted packet) is configured as a security zone-member.

Workaround: Remove the **zone-member security zone_name** command from the crypto outside interface. This will prevent the application of the Zone Firewall policy on clear-text traffic from the problem interface and other firewall security zones.

- CSCsd76813

Symptoms: On a Cisco RPM-XF Router, policing succeeds only on the last interface when the same policy-map is applied to several interfaces.

Conditions: This symptom has been observed when the same policy map is applied to several interfaces.

Workaround: Create several policy-maps with different names and apply them to the interfaces instead of applying the policy-map with the same name to all interfaces. It is also observed that the condition is rectified after some time. This time cannot be estimated. The police parameters for this situation are not exactly understood.

- 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.

- CSCsd80754

Symptoms: The HSRP Active-Router does not respond to ARP request for the virtual IP address.

Both HSRP routers have the correct HSRP and ARP entry during this problem.

Issuing the **clear arp** command on the HSRP standby router does not resolve the problem.

Conditions: This problem may occur where the same HSRP virtual IP address exists on different HSRP groups on different routers.

Workaround: Configuring "no standby redirects" will prevent this from occurring.

- 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.

- CSCse20809

Symptoms: IKE SA processing stops at CONF_XAUTH state although the extended authentication (Xauth) username and password are configured on EzVPN Remote correctly.

Conditions: This symptom has been observed when load balancing is configured on a Cisco VPN 3000 Series Concentrator.

Workaround: There is no workaround.

Wide-Area Networking

- 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.

- CSCsd71360

Symptoms: PPP Multilink fragment loss occurs as the result of premature lost fragment timeouts. This can be seen in the lost fragment count in the output of the **show ppp multilink** command, as well as debug traces produced by the **debug ppp multilink events** command.

Conditions: This symptom has been observed with Cisco IOS Release 12.2(28)SB and Release 12.4(6)T, but not with Cisco IOS Release 12.2(27)SBC2 or Release 12.4(4)T.

Workaround: Configure the **ppp timeout multilink lost-fragment 1** command under the Multilink interface or the Virtual-Template interface corresponding to the multilink bundle.

- 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(6)T11

Cisco IOS Release 12.4(6)T11 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T11 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

IP Routing Protocols

- 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>

- CSCek76776

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

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

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

- CSCsi17020

A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

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

- CSCsi68963

Symptoms: A Cisco 7200P router crashes while removing an IPv6 Protocol Independent Multicast (PIM) bootstrap router (BSR) candidate from the configuration.

Conditions: This symptom is observed when an IPv6 PIM BSR candidate is unconfigured.

Workaround: There is no workaround.

Further Problem Description: After RP information is learned on all of the routers, delete the ACL first and then the BSR candidate.

- CSCsj85065

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

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

- CSCsk40676

Symptoms: The inside interface of a Cisco router that is running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Conditions: This symptom is observed when LZS compression is used on a Windows Vista client.

Workaround: Disable LZS compression.

- CSCsk42759

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

- CSCsl62609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

Resolved Caveats—Cisco IOS Release 12.4(6)T10

Cisco IOS Release 12.4(6)T10 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T10 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCek50783

Symptoms: “Enqueue to process level” message is seen in logs.

Conditions: This symptom has been observed in Cisco IOS Release 12.4T and 12.4 (4)XD2. No debugs are enabled.

Workaround: There is no workaround.

- CSCsk62253

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml>

- CSCsk70446

Cisco IOS emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

A traceback appears after the error message. This traceback is encountered with long URLs.

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

IP Routing Protocols

- CSCsh84102

Symptoms: The following symptoms may occur:

- Some DMVPN spokes become unreachable and a loop appears in a traceroute.
- When you enter the **show adjacency details** command on the hub, the output shows that the adjacency rewrite information for a problematic spoke is the same as for another spoke.
- There is an inconsistency between the NHRP cache and the adjacency for the problematic spoke.

Conditions: These symptoms are observed in a DMVPN configuration when the hub has CEF enabled.

Workaround: Disable CEF on the hub.

- CSCsj09838

Symptoms: When the BGP session between a Route Reflector (RR) and PE router flaps, the RR may no longer send some routes to the PE router.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsi85222. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi85222>. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **clear ip bgp * all in** command on the PE router to retrieve all routes from the RR.

- CSCsl01874

Symptoms: Cisco IOS configured with the Dynamic Multipoint VPN (DMVPN) feature allows stale tunnel endpoint entries to remain in the system. This occurs even though the Next Hop Resolution Protocol (NHRP) cache entry does not exist.

Conditions: When a spoke registers with a changed tunnel IP address (overlay address), there will be two overlay addresses mapped to same NBMA address on the hub. As a result when the NHRP mapping for the stale overlay address (old tunnel address) expires on the hub, the tunnel endpoint entry is not deleted, resulting in a stale tunnel endpoint entry.

Workaround: There is no workaround.

Miscellaneous

- CSCsg76519

Symptoms: An RSP may crash when you enter the **clear counters** command.

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.4 when you enter the **clear counters** command after the termination of voice calls that were made with PA-VXC-2TE1 port adapters.

Workaround: There is no workaround.

- 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>.

- CSCsi80057

Symptoms: Conditional default origination into RIPv2 does not work correctly in the following scenarios:

1. When the watched network is not present, the default route is not deleted from the local RIP database. This causes the router to still send the default route.
2. When the watched network is present, the default route is not added to the local RIP database. This causes the router to not send the default route.

The default behavior can be seen at the following link:

http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_rip.html#wp1011008

Conditions: This symptom is observed if the **default-information originate route-map map-name** router RIP configuration command is used in order to generate a default route only when the watched network is present.

Workaround: There is no workaround.

- CSCsi81891

Symptoms: RTP packets get transmitted when the mode is recvOnly and inactive.

Conditions: This problem is observed on both the Cisco 2800 and the Cisco 3800 platforms that are running Cisco IOS interim Release 12.4(13.9).

Workaround: There is no workaround.

- CSCsi92614

Symptoms: Virtual Switch Interface (VSI) process stack overflow causes card to crash.

Conditions: Occurs when connection goes into condition alarm state while multicast is configured and it is managed by Operation and Maintenance (OAM).

Workaround: There is no workaround.

- CSCsj46178

Symptoms: A Cisco AS5850 responds with a 500 Endpoint Unknown to a CRCX for an endpoint on a channelized T3 card. The endpoint otherwise responds normally to AUEP command.

Conditions: This symptom is observed on a Cisco AS5850 that is controlled via MGCP, and the **endpoint naming t3** command is configured on the router in either global MGCP configuration or MGCP profile.

Workaround: Do not configure the **endpoint naming t3** command. Use t1 endpoint naming instead.

- CSCsj64230

Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

Workaround: There is no workaround.

- CSCsj74812

Symptoms: A router running Cisco IOS may reload unexpectedly.

Conditions: Occurs when using **show** commands on an exec session that has been established through one of the integrated modems on a WIC-AM or WIC-2AM.

Workaround: There is no workaround.

- CSCsj95947

Symptoms: The following message is seen on the router:

```
*Aug 6 16:34:47.188: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC=
0x8005EC50, -Traceback= 0x809971F4 0x809B9C2C 0x809DD8A4 0x8005EC50 0x800651E4
0x800652A8 0x809E42D4 0x809C4A38 0x800652EC 0x809C4BA0 0x809E42D4 0x80A0854C
0x800DB8C0 0x800DEE48
```

Conditions: The conditions under which this symptom occurs are not known at this time.

Workaround: There is no workaround.

- 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 and allow the GRE traffic.

- CSCsk26973

Symptoms: A router that is running NHRP leaks memory when many incomplete cache entries are created. The incomplete cache entries can be verified by typing the **show ip nhrp** command and looking for “type incomplete”. The memory leaked can be seen by examining the output of the **show chunk** command and looking for “NHRP Cache”.

Conditions: This symptom could occur when traffic to nonexistent or non-responding addresses are forwarded by the router over the DMVPN/NHRP cloud.

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>

- CSCsk75098

Symptoms: A Cisco 7200 NPE-G2 router with a VSA encryption card, terminating IPsec EasyVPN Dynamic Virtual Tunnel Interfaces, exhibits high CPU utilization during IKE and IPsec rekeys, potentially causing some tunnels to go down.

Conditions: This symptom is observed on a Cisco 7200-G2 router with a VSA card, acting as an IPsec HUB, terminating EasyVPN DVTI remote-access IPsec tunnels into VRFs. At high tunnel scale (more than 1000 tunnels), the CPU can spike close to 100 percent during IKE and/or IPsec rekey, potentially causing traffic and tunnels to drop.

Workaround: Do not use more than 1000 RA EasyVPN DVTI tunnels on a Cisco 7200. Or switch to Legacy EasyVPN tunnels (with dynamic crypto maps).

- CSCsk99530

Symptoms: The MPLS forwarding table has an untagged outgoing entry for a VPNv4 prefix in a CSC case.

Conditions: This is an LDP/IGP (OSPF etc.) based CSC-PE. The VPNv4 prefix shall have a local/redistributed (PE-CE OSPF etc.) path as well as an iBGP path. If the CE path is toggled and then there is a LABEL ONLY change from the iBGP neighbor, the issue will be seen. BGP will end up programming “Untagged” for the local/redistributed prefix, overwriting what is given by LDP.

Workaround: There is no real workaround. To clear the problem, issue a **clear ip route** command for the vrf-prefix in question. If there are redundant paired PEs, make sure to clear the problem on both routers with the **clear ip route** command.

- CSCsl14635

Symptoms: T38 negotiation is failing for an incoming UPDATE request that has a T38 offer.

Conditions: This symptom occurs when the voice gateway is running Cisco IOS Release 12.4(15)T and is processing incoming Session Initiation Protocol (SIP) calls. When the SIP call is active and an UPDATE request is received that contains a T38 offer, the UPDAE request is rejected. The switchover from voice to fax fails.

Workaround: Fax over T38 works fine when midcall INVITE is used for T38 negotiation.

- CSCsI90470

Symptoms: Cisco Intrusion Prevention System (IPS) does not inspect intra-zone traffic when router is configured with zone-based firewall.

Conditions: Occurs on routers using Cisco IOS IPS and zone-based firewall features.

Workaround: Create a separate zone for each interface. Use an appropriate naming scheme to assist in identifying which interfaces would normally be in the same zone if not for this issue. Create service policies that allow all traffic between the interfaces that were previously in the same zone.

Note: This workaround only works on routers running Cisco IOS Release 12.4(15)T and later releases.

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(6)T9

Cisco IOS Release 12.4(6)T9 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T9 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

IP Routing Protocols

- CSCei93768

Symptoms: A Cisco router that is configured for BGP may crash and generate the following error messages:

(Note that the hex values of tracebacks and other parameters that are part of the error messages will vary with different occurrences of the symptom).

```
%SYS-2-NOTQ: unqueue didn't find 4552953C in queue 454BE738
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC
40C3BA10 40C3CCE0
%SYS-2-NOTQ: unqueue didn't find 455294EC in queue 454BE690
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC
```



```

40C3BA10 40C3CCE0CMD: 'end'

%SYS-5-CONFIG_I: Configured from console by console
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header,
chunk 45519C14 data 4552953C chunkmagic 15A3C78B chunk_freemagic 0
-Process= "Check heaps", ipl= 0, pid= 6
-Traceback= 4063C5FC 4063C788 4065A9D0
chunk_diagnose, code = 2
chunk name is IP RDB Chunk

current chunk header = 0x0x4552952C
data check, ptr = 0x0x4552953C

next chunk header = 0x0x4552957C
data check, ptr = 0x0x4552958C

previous chunk header = 0x0x455294DC
data check, ptr = 0x0x455294EC

```

Conditions: This symptom is observed mostly with configuration changes that involve the **bgp dmzlink-bw** command for a BGP IPv4 address family, but in very rare cases, the symptom may also occur on other situations.

Workaround: There is no workaround.

- CSCsg55591

Symptoms: When there are link flaps in the network, various PE routers receive the following error message:

```
%BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
155:14344:10.150.3.22/32 from 10.2.2.1
```

Or, a local label is not programmed into the forwarding table for a sourced BGP VPNv4 network.

Conditions: These symptoms are observed when an iBGP path for a VPNv4 BGP network is present, and then a sourced path for the same route distinguisher (RD) and prefix is brought up.

Workaround: Remove the iBGP path. Note that when the sourced path comes up first, the symptoms do not occur.

Alternate Workaround: Use different RDs with the different PE routers. When the RD and prefix do not match exactly between the iBGP path and the sourced path, the symptoms do not occur.

- CSCsj10772

Symptoms: The TTL of a CNAME will be zeroed on a DNS reply after passing through a Cisco router that is configured for Network Address Translation (NAT).

Conditions: This symptom is observed on a Cisco router that is configured for NAT that is running Cisco IOS Release 12.4 or 12.4T. Only CNAME records are affected.

Workaround: Use static NAT translations with the keyword “no-payload”.

- CSCsj39538

Symptoms: Router tracebacks and then crashes during deconfiguration (removal) of VRF. The following message was seen prior to crash:

```
-Process= "IP RIB Update", ipl= 3, pid= 68
-Traceback= 609538D8 60D1B8B4 612B2838 612588C8 61258CD4 6125E61C 6125ED04 6125EF30
61261CDC 6125A14C 61265A08 6126BE10 6097CF00 609547D8 609548B8
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x609538FC
Conditions: No specific conditions are known to cause this fault.
Workaround: There is no workaround.
```

Miscellaneous

- CSCdz55178

Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                                000000000111111111122222222333^
                                12345678901234567890123456789012|
                                                                |
                                                                PROBLEM
                                                                (Variable Overflowed).
```

Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- 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>.

- CSCsd27617

Symptoms: IKE negotiation fails with a wrong group preshared key.

Conditions: This symptom is observed on a Cisco router that has an eight character key such as "cisco123" that is defined under the EzVPN group configuration and occurs after you have entered the **password encryption aes** command.

Workaround: To prevent the symptom from occurring, do not use an eight character key under the EzVPN group. After the symptom has occurred, re-enter the group and key.

- 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>.

- CSCse56800

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>.

- CSCsg42246

Symptoms: High CPU use may occur in the “IP Background” process, and the router may reload unexpectedly.

Conditions: This symptom is observed on a Cisco router that is configured for RIP and that receives a RIP host route that is subsequently replaced by a route that is dynamically assigned to an interface. For example, this situation may occur on a PPP interface that has the **ip address negotiated** command enabled.

Workaround: Use a route map to block the advertised route.

- 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.

- CSCsi92079

Symptoms: If an access control list (ACL) is used for a destination only prefix, a fatal error is declared and shuts down optimized edge routing (OER). For destination only traffic classes, prefix-list should be used, not ACL or access control entry (ACE).

Conditions: This behavior is observed on Cisco IOS Release 12.4(11)T and later releases at this time.

Workaround: Use prefix list instead of ACL/ACE for destination only traffic classes. For example:

- use prefix list for a traffic class 100.1.1.0/24
- use ACE for traffic class 100.1.1.0/24 DSCP af11

- CSCsj43861

Symptoms: EzVPN hardware client will not attempt to connect to the same peer or the next peer after QUICK MODE failure during IKE.

Conditions: This symptom is observed when EzVPN hardware client remains in SS_OPEN state after the failure of QUICK MODE.

Workaround: Clear the EzVPN session.

- 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.

- CSCsk33780

Symptoms: Compressed Real-Time Protocol (cRTP) shows errors and Low Latency Queuing (LLQ) shows drops from default queue although there is no traffic to match it.

Conditions: This problem can be seen under load of MPPP bundle of several serial interfaces with LLQ and cRTP enabled.

Workaround: There is no workaround.

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(6)T8

Cisco IOS Release 12.4(6)T8 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T8 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCsg05378

Symptoms: A router may hang or crash because of memory corruption when HTTP is being accessed.

Conditions: This symptom is observed on a Cisco router when IPS is enabled. Other conditions may trigger the symptom too.

Workaround: When IPS triggers the symptom, disable IPS.

- 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.

IP Routing Protocols

- 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.

- CSCek30198

Symptoms: The nexthop tracking information is not updated properly at the required time.

Conditions: This symptom is observed when BGP next hops are modified or deleted.

Workaround: There is no workaround. You must wait 10 minutes for the update to occur.

- 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

- CSCej59405

Symptoms: The output of **show running-config** command does not show a correct parent-child relationship between the control plane and its underlying service policy.

Conditions: This symptom is observed on a Cisco router that has control-plane features such as policing and port-filtering enabled.

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.

- CSCsd43903

Symptoms: A Cisco router may experience memory leaks in the Crypto IKMP process when using certificates for Internet Security Association and Key Management Protocol (ISAKMP) for peer authentication.

Conditions: This symptom has been observed on Cisco IOS Release 12.2(18)SXE5 and Release 12.4(9)T2. This symptom is platform independent.

Workaround: There is no workaround to prevent the leak and the only way to recover is to reboot the device.

- 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.

- 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>.

- CSCse67995

Symptoms: A memory leak may occur in the “Crypto IKMP” process.

Conditions: This symptom is observed when you use certificates for IKE authentication.

Workaround: Use preshared keys for IKE authentication.

- CSCsg10134

Symptoms: A router crashes when PPPoEoA sessions are torn down.

Conditions: This symptom is observed when the maximum number of class-map instances are configured on the router.

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.

- 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>

- CSCsg83326

Symptoms: IPSec does not function when IPv6 is enabled, preventing all crypto-related functions from properly operating.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T and that has IPv6 enabled.

Workaround: There is no workaround.

- CSCsg92700

Symptoms: All GLBP IPv6 group members remain in the active state at all times, and no GLBP IPv6 protocol information is passed between group members.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(11.4)T or a later release.

Workaround: There is no workaround.

- 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.

Workaround: Configure reverse SSH by entering the **ip ssh port portnum rotary group** command.

- 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.

- CSCsh35269

Symptoms: When using MTP on a Cisco IOS router, there could be RTP ports and RTP SPI call legs hanging. Over time, the hanging RTP ports can accumulate and cause the router to run out of RTP ports, so MTP calls will fail.

Conditions: This symptom has been observed when using software MTP for supplementary services or when there is a high number of calls per second (CPS).

Workaround: Reload the router to release the hanging ports.

- 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.

- CSCsh84171

Symptoms: A router that is configured with an HWIC-ADSL-B/ST crashes because of memory corruption and generates the following error message:

```
%SYS-3-OVERRUN: Block overrun at 3F379450 (red zone 2A2A2A2A)
```

Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.4T.

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>.

- CSCsi09530

Symptoms: If the **authenticate register** command is configured under the **voice register global** command, CME SIP failed to registered.

Conditions: The **authenticate register** command is configured under the **voice register global** command when CME is acting as a registrar.

Workaround: Disable the **authenticate register** command under the **voice register global** command.

Further Problem Description: In registrar functionality, CME challenges an inbound register request with a 401 response. If the **authenticate register** command is configured under the **voice register global** command, the Registering Endpoint then ends a Register Request with Credentials. The Gateway Stack is not processing this request and is dropping it.

- CSCsi10157

Symptoms: When you associate and then disassociate a VRF from a tunnel source interface, a DMVPN spoke may crash.

Conditions: This symptom is observed only when a VRF is configured on a tunnel interface.

Workaround: There is no workaround.

- 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.

- CSCsi59685

Symptoms: One-way audio may occur and DTMF digits may not function.

Conditions: This symptom is observed on a Cisco gateway such as a Cisco AS5400 after a SIP transfer has occurred.

Workaround: Enter the **no voice-fastpath disable** command to resolve the one-way audio issue. There is no workaround for the DTMF issue.

- CSCsi60004

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsi67127

Symptoms: There are several symptoms:

1. After “INPUT/OUTPUT Queue Full Error” error messages have been generated on a router that has an IPSec interface, traffic is no longer processed. The output of the **show crypto engine accelerator statistic** command shows the following:

```
...
Input Queue Full Error      = 50
Output Queue Full Error    = 2811
...
```

2. The ISAKMP process is stuck. Look for “Crypto IKMP” in the output of the **show processes** command. Identify the process ID (PID). When you execute the **show processes pid** command for the Crypto IKMP PID several times in a row, you can see that the ISAKMP process is stuck when the value “Invoked” does not increase even though IKE has negotiated SAs.

Conditions: This symptom is observed on a Cisco 850 series, Cisco 870 series, Cisco 1800 series, and Cisco 1810 series.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reboot the router to clear the faulty condition.

- 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>

- CSCsi70787

Symptoms: A router may reset and generate a crashinfo file when memory that was allocated by a dead process is freed by another process.

Conditions: This symptom is observed on an RPM-XF-512 that runs Cisco IOS Release 12.4T but is not platform-specific.

Workaround: There is no workaround.

- CSCsi70791

Symptoms: A Cisco router can experience a memory corruption crash related to encryption.

Conditions: This symptom has been observed when the **memory lite** global configuration command is disabled.

Workaround: Enable the memory allocation lite (malloc_lite) feature by using the **memory lite** command.

- CSCsi80749

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>

- CSCsi83259

Symptoms: The 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 on a Cisco RPM-XF-512 that runs Cisco IOS Release 12.4(6)T5 but is not platform-specific.

Workaround: Enter the **clear ip route** command for the prefix in the VRF.

- 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.

- CSCsj32707

Symptoms: A “SIP UPDATE” message from a Cisco CallManager or SIP Proxy Server with a “Cseq” value of 0 may be rejected or considered invalid by A Cisco gateway.

Conditions: This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.4(9)T4 or a later release and that is connected to a SIP endpoint.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(9)T3.

- CSCsj34083

Symptoms: Packets in traffic queues that are below their configured threshold may be dropped.

Conditions: This symptom is observed on a Cisco 877 and Cisco 1801 that run Cisco IOS Release 12.4(9)T3 when one of the queues trespasses its threshold. Note the following scenarios:

- When congestion is present, traffic that exceeds its threshold on a CBWFQ service class causes drops on the LLQ classes although the traffic that is associated with the LLQ classes is below the associated threshold.
- When best-effort bandwidth exceeds its threshold, LLQ traffic is discarded although it is below its own threshold.
- When there is no congestion, the router operates as expected.

Workaround: There is no workaround.

Further Problem Description: Note that the symptom does not occur on a Cisco 878 and Cisco 1803.

- CSCsj61988

Symptoms: A router may crash when you attempt to establish a session between a Cisco Unity client and a Cisco Unity server.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(6)T8 and occurs because of memory corruption.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsi40766

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

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

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

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

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

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

Wide-Area Networking

- 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 Serial12/0
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

- CSCsf30411

Symptoms: In an L2TP dialout configuration, when a failover occurs and when limit and priority options are specified, the output of the **show vpdn** command may be incorrect. This situation causes the limit option to be unusable.

Conditions: This symptom is observed when limit and priority options are enabled on the LNS and when a ping is made from the LNS to two LACs to check if the limit option functions. The session should be the same as that of the limit, but is more than the specified limit.

Workaround: There is no workaround.

- CSCsi27449

Symptoms: A Non-Facility Associated Signaling (NFAS) configuration with a back-to back PRI connection may fail and an “L3_GetUser_NLCB EVENT 0X2 No NLCB 2” error message may be generated, that is, a ping from the client to the router may fail.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.11) when an interface is configured as a dialer interface. The symptom may also affect Release 12.4T.

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(6)T7

Cisco IOS Release 12.4(6)T7 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T7 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCse23950

Symptoms: A router hangs on a regular basis producing the following traceback:

```
%SYS-2-NOTQ: unqueue didn't find 0 in queue 82E19A74
-Process= "<interrupt level>", ipl= 2
-Traceback= 0x80836CE8 0x814DC7F0 0x814EBE5C 0x816DF1F0 0x816DF2A8 0x816DEF74
0x816DE8D4 0x80076750 0x8072CFA0 0x8072D10C 0x803B128C 0x80143E5C 0x801383B4
0x8013AB0C 0x8013D6E0 0x8037DF44
```

Conditions: This symptom is observed on a router that is acting as an EzVPN Client. From the traceback, it seems that the BVI interface is involved in the crash.

Workaround: Disable bridging or HW encryption.

- CSCsg00102

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- 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

Symptoms: EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

Conditions: This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGp session on a CE router. This occurs typically in the following inter-autonomous system scenario:

```
ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2
```

Workaround: Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
  address-family ipv4 vrf one
  neighbor 1.0.0.1 remote-as 100
  neighbor 1.0.0.1 activate
  neighbor 1.0.0.1 route-map FILTER in
  exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
  set extcomm-list 100 delete
!
```

- 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

- CSCds25257

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

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

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

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

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

- 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>.

- 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.

- CSCek61974

Symptoms: You may be able to configure a minimum receive interval as short as 1 ms, which may cause problems on the router.

Conditions: This symptom is observed on a Cisco router that supports Bidirectional Forwarding Detection (BFD). Note that a minimum receive interval shorter than 50 ms is not supported in Cisco IOS software images.

Workaround: Configure a minimum receive interval of 50 ms or longer.

- CSCsb15138

Symptoms: The following error messages may be generated on a gateway that functions in a configuration in which 80 channels are processed by a VXML Server, and the call may be dropped:

```
//-1//HTTTPC:/httpc_streaming_create: attempt to create a session with id 699
while this id is in use

//2144684/0BCEFBA9AA28/VXML:/vxml_media_done:

CALL_ERROR; fail with vapp error 2, protocol_status_code=0

//2144684/0BCEFBA9AA28/VXML:/vxml_media_done:
```

```
CALL_ERROR; *** error.badfetch.http.0 event is thrown
```

Conditions: This symptom is observed rather rarely on a Cisco AS5400 gateway when the HTTP client session IDs range from 1 to 2048 because of the socket limit per Cisco IOS process. The error messages are generated when the HTTP client attempts to create a new session with the same ID as an old session that is still in use. In this situation, only a benign warning message should be generated, and the call should be accepted. If an HTTP streaming session remains in use for a long time and the traffic load of the gateway is high, the symptom is more likely to occur.

Workaround: Configure an event handler as in the following example:

```
<catch event="error.badfetch.http.0">
<!-- Actual event handler goes in here -->
</catch>
```

If this is not an option, the symptom may be mitigated by disabling IVR streaming mode via the **ivr prompt streamed none** command.

- CSCsc33783

Symptoms: When using Object Tracking in Cisco IOS, some configuration may be lost on reload depending on the configuration of the object tracking references. Objects are parsed in sequential order so if one tracked object references a second tracked object of higher number then that second object will not be defined when the first object is initialized on reload.

Conditions: This symptom occurs when using Object Tracking in Cisco IOS.

Workaround: Always use a higher numeric object tracking ID for the parent object.

- 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>

- 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>.

- 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/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

- CSCse31572

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

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T. The symptom could occur in Release 12.4.

Workaround: There is no workaround.

- CSCse40276

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>

- CSCse90464

Symptoms: When a router receives IP fragments that match an access control list (ACL), a spurious memory access may occur and the router may crash.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T, Release 12.4, or Release 12.4T when an extended ACL is configured and when the router receives IP fragments that match the ACL.

Workaround: If the Turbo ACL feature is an optional feature on the router, disable the Turbo ACL feature by entering the **no access-list compiled** command. If the Turbo ACL feature is not an optional feature on the router, that is, it is always enabled, there is no workaround. On the Cisco RPM-XF there is no workaround.

- 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>

- CSCsf30058

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>

- CSCsg39167

Symptoms: A router crashes because of memory corruption with the following message:

```
%SYS-3-OVERRUN: Block overrun at E73C97D0 (red zone 55555555).
```

Conditions: This symptom occurs on a Cisco 1800 router that is running Cisco IOS Release 12.4T images and has a HWIC-ADSL-B/ST card.

Workaround: There is no workaround.

- CSCsg59037

Symptoms: Cisco 851 and 871 routers have no way to remotely upgrade the ROMMON firmware image.

Conditions: Cisco IOS versions for the Cisco 851 and 871 routers did not provide a mechanism to remotely upgrade the ROMMON firmware image.

Workarounds: Cisco IOS Release 12.4(11)T1 for the Cisco 851 and 871 router introduces the command **upgrade rom-monitor file** which allows the ROMMON firmware image to be remotely upgraded. Please consult this link for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tcf_r/cf_13ht.htm#wp1032550

- CSCsg61748

Symptoms: After heavy traffic on a VTI interface with HW encryption (about 15 Mb/s), the queue of the interface is stuck.

When the symptom happens, Input/Output Queue Full Error of “show crypto engine accelerator statistic” is increased.

Conditions: This symptom is observed on a router that is running Cisco IOS Releases 12.4(6)T2, 12.4(6)T5, or 12.4(9)T1 that use HW encryption.

Workaround: There is no workaround.

- CSCsg76715

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

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

- The inserted ACE has a destination prefix length of 0, that is, is has an “any” statement instead of a destination address.
- The ACL already has another ACE with the same SRC prefix length and an destination prefix length that is greater than 0 (that is, other than an “any” statement), and the inserted ACE has a lower sequence number than this other ACE.
- The other ACE with a destination prefix length that is greater than 0 is deleted before you delete the inserted ACE.

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

Alternate Workaround: Delete the complete ACL.

- CSCsh20336

Symptoms: A spoke may be unable to connect or reconnect to a hub because there may not be a crypto socket.

Conditions: This symptom is observed in a DMVPN Hub-to-Spoke environment.

Workaround: Remove the static NHRP entry from the tunnel interface that connects the spoke to the hub, and reapply the static NHRP entry.

- CSCsh31605

Symptoms: In a dial backup scenario with backup EzVPN over an asynchronous or dialer interface, EzVPN fails to kickoff the asynchronous or dialer interface intermittently. Dial backup EzVPN cannot be brought up always. It works intermittently.

IKE request packet in failure cases is dropped with the following error:

```
*Oct  5 07:39:22.187: EZVPN(backup): New State: READY
*Oct  5 07:39:22.187: EZVPN(backup): Current State: READY
*Oct  5 07:39:22.187: EZVPN(backup): Event: CONNECT
*Oct  5 07:39:22.187: EZVPN(backup): No state change
*Oct  5 07:39:22.187: ISAKMP:(0):receive null address from sa_req (local
0.0.0.0, remote 10.175.161.41)
*Oct  5 07:39:22.191: ISAKMP: Error while processing SA request: Failed to
initialize SA
*Oct  5 07:39:22.191: ISAKMP: Error while processing KMI message 0, error 2.
*Oct  5 07:40:03.551: ISAKMP:(2018):purging SA., sa=841CC6D0, delme=841CC6D0
```

Conditions: This symptom occurs in a dial backup scenario with backup EzVPN over an asynchronous or dialer interface.

Workaround: There is no workaround.

- CSCsh37414

Symptoms: EzVPN leaks some memory with the fix of CSCsg94570. It can take a long time for the box to run out of memory causing a reload.

Conditions: This symptom is observed when EzVPN leaks memory.

Workaround: There is no workaround.

- 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-ROUTE LIMIT (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.

- CSCsh50275

Symptoms: In a DMVPN setup with spoke having overlapping ISAKMP profiles and DPD enabled, IKE quick mode fails due to ISAKMP profile mismatch. After IKE SA expiry, the IKE SA rekey triggered by ISAKMP keepalives does not use any ISAKMP profile while initiating the SA. With overlapping ISAKMP profiles present, the IKE SA might end up attaching to the incorrect ISAKMP profile instead of the one configured on the corresponding tunnel interface and the one used by original IKE SA, subsequently causing the quick mode to fail due to profile mismatch. The only way to bring them out from that stage is by clearing Phase 1 SA.

Conditions: This symptom occurs during DMVPN testing.

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>.

- CSCsi04183

Symptoms: A router that is configured as an EasyVPN client is not able to auto connect to the EasyVPN server using its saved Xauth username/password.

Conditions: This symptom is observed when the router is powered-up or when the ISAKMP re-keying happens.

Workaround: Manually execute the **crypto ipsec client ezvpn xauth** command in the router console and enter the respective username/password.

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:

- 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.

- CSCsg00102

Symptoms: In Cisco IOS Release 12.4(9)T, the TCP stops accepting new connections after a few days of SSLVPN running in the router. The **debug ip tcp transaction** command shows the error with connection queue limit reached. When the problem happens, the **show tcp bri all** command shows five connections in CLOSED state.

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

Workaround: Enter the **clear tcp tcb *** command. This command will clear all the TCP connections on the router.

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.

- CSCek60025

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

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

Workaround: There is no workaround.

- CSCek62099

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

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

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

Alternate Workaround: Disable MLP.

- CSCek67875

Symptoms: During a test of a B-Channel Maintenance Procedure (BCAC), an incoming SERVICE message is not printed with the correct channel.

Conditions: This symptom is observed when a collision occurs between a SERVICE message and a SETUP message.

Workaround: There is no workaround.

- 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.

- CSCsh85902

Symptoms: For normal ISDN call and disconnecting the call, a DISCONNECT message will be issued. The contents of this DISCONNECT message will be replaced with the one that is explicitly configured. This configured message has an invalid facility component and hence the receiving side should send facility reject component which is not seen here (missing).

Conditions: This symptom happens with Cisco IOS Interim Release 12.4(12.15)T. This is happening only for Interface PRI. This is seen for Cisco IOS Release 12.4 mainline & Release 12.4T.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(6)T6

Cisco IOS Release 12.4(6)T6 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T6 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

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

- 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

- 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.

- CSCse81684

Symptoms: A router running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:

```
---- Partial decode of process block ----
Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540
```

Conditions: This symptom has been seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

Workaround: Prevent the router from receiving a fragmented skinny packet by ensuring the path MTU between the call manager server and the router is large enough. Usually skinny packets aren't larger than 800 bytes.

- CSCse97264

Symptoms Two or more udp NAT translations relating to different requests may be assigned with the same pair INSIDE_GLOBAL_IP:PORT

Conditions This problem is observed on cisco2800 platform running 12.3(11)T9, when more than one IP-Phones try to register themselves through a router configured with NAT Overload

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).

- CSCsg22426

Symptoms: A router running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:

```
---- Partial decode of process block ----
```

```
Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540
```

Conditions: This is seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

Workaround: Prevent the router from receiving a fragmented skinny packet by ensuring the path MTU between the call manager server and the router is large enough. Usually skinny packets aren't larger than 800 bytes.

Miscellaneous

- 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.

- 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.

- 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.

- 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.

- CSCsd23454

Symptoms: The main issue is `crypto_ipsec_sa_lookup_insert()` routine holds the memory for spi allocation.

Conditions: Several reasons contribute to this problem:

- ike allocates spi at MM1. This design was originally for async spi allocation. Since the allocation scheme has changed to sync scheme, it is ok to move back to qm phase. The transient spi handle problem can be observed with mis-match ike/ipsec proposal or in vti scenario if we only bring up one node ipsec. Both cases will continue allocating the spi at MM1 and waiting for 864 seconds timer expired to clean up spi transient handle. Since it takes 12 to 13 minutes to release the handle, and ike continue retrying MM1 negotiation. The memory can ramp up tremendous high.
- Some transient spi handles do not release at the right time. When ah and esp are used, both allocate spis. The spi mature routine is used to release spi transient handle when the ipsec sa is created successfully. The code logic missed to clean up some of transient spis handle for different transform. It leaves there until it expires.
- When ike negotiation is failed, the current code ike does not have scheme to notify ipsec in order to clean up the associated spi table. It leaves there for 864 seconds to expire. The expiration timer is set to too long. It will hold the memory due to negotiation failure.

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.

- 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.

- 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.

- CSCsd91454

Symptoms: Voice traffic is dropped in one direction due to IPHC IPCRC error.

Conditions: The problem is found some time after the voice call has been established. When the problem is occurring, the logs show IPHC error messages.

Workaround: Use process switching.

- 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.

- CSCse04136

Symptoms: Router crashing with traceback.

Conditions: This symptom has been observed when using a Cisco 7200 router to send traffic using IXIA after applying a crypto map feature.

Workaround: There is no workaround.

Further Problem Description: The crash was obtained when testing TED feature in a Cisco 7200 routers using IXIA. While sending packet to initiate IPSec tunnel, the router got crashed with traceback.

- 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.

- 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.

- 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.

- CSCsf05693

Symptoms: A router may unexpectedly reload after reporting “Unexpected timer” errors similar to:

```
Aug 6 17:29:16.908 GMT: %SIP-3-BADPAIR: Unexpected timer 19
```

```
(SIP_TIMER_NOTIFY_RECEIVE_DIGIT) in state 10 (STATE_DEAD) substate 0 (SUBSTATE_NONE)
```

Conditions: The router must be configured for SIP.

Workaround: There is no workaround.

- CSCsf16536

Symptoms: A Cisco IOS router may experience a unexpected reload.

Conditions: This problem occurs when the router has IPS (Intrusion Prevention Systems) configured, and one or more attack signatures has the denyFlowInline action enabled.

Workaround: The workaround is to not enable the denyFlowInline action for any IPS signatures.

- 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.

- 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>.

- CSCsg22426

A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

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

- CSCsg39961

Symptoms: A router may unexpectedly reload when trying to send a PKI request to a CA.

Conditions: The router must be configured with crypto PKI trustpoints.

Workaround: Because this is a 1 byte redzone overrun, the following will prevent the crashes, and will display error messages instead.

First, to prevent the usage of chunks, configure "no memory lite". Second, configure "exception memory ignore overflow processor" to correct the redzone overrun.

- 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

- 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.

- 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.

- 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.

- 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.

- CSCsf96318

Symptoms: 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.

Resolved Caveats—Cisco IOS Release 12.4(6)T5

Cisco IOS Release 12.4(6)T5 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T5 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

TCP/IP Host-Mode Services

- CSCsd74139

Symptoms: HTTP errors occur while accessing a Win2003 Web Server.

Conditions: This symptom has been observed with a Cisco IOS Voice gateway running Cisco IOS Release 12.4(6)T accessing a Win2003 HTTP web server under heavy load. Cisco IOS Voice has **ip http client connection persistent** disabled.

Workaround: There are two possible workarounds:

1. Switch to a Win2000 HTTP web server.
2. On a Win2003 server, set "TcpTimedWaitDelay" to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

- CSCsg26634

Symptoms: CPUHOG can occur when running lots of BGP connections.

Conditions: This symptom has been observed with a Cisco IOS Voice gateway running Cisco IOS Release 12.4(6)T.

Workaround: There is no workaround, though the symptom was quickly found and repaired.

Resolved Caveats—Cisco IOS Release 12.4(6)T4

Cisco IOS Release 12.4(6)T4 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T4 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCea36491

Symptoms: When entering the router's configuration mode or similar 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: This symptom has been observed when sending 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 SNMP configuration traps by entering the **no snmp- server enable traps config** global configuration command.

- 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: 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 sent and when an AAA server is slow or unreachable.

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.

- 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.

IP Routing Protocols

- CSCek42700

Symptoms: A network and host-based configuration download over serial HDLC with an IP address obtained via SLARP fails.

Conditions: This symptom has been observed with a router that has no startup- configuration (after using the **write erase** command) but is staged for autoinstall over a serial link. An IP address is obtained, but the download fails with the following error message:

```
%Error opening tftp://255.255.255.255/network-config (Socket error)
%Error opening tftp://255.255.255.255/cisconet.cfg (Socket error)
```

Without this feature, router deployment with automatic configuration download at remote sites over serial interface is not possible.

Workaround: Use another method of autoinstall if possible, or pre- configure the router before deployment.

- 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.

- 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.

- 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.

- 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-adviservicesk9-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.

- CSCse68877

Symptoms: A label mismatch may occur between the CEF table and the BGP table, and a new label may not be installed into the CEF table.

Conditions: This symptom is observed after a BGP flap has occurred on a Cisco router that is configured or MPLS VPN but that does not function in an inter-autonomous system and that does not have multiple VRFs.

Workaround: There is no workaround. After the symptom has occurred, enter the **clear ip route** command for the affected VRF.

- CSCsf11052

Symptoms: Error messages are seen such as the following example:

```
%NHRP-3-PAKREPLY: Receive Resolution Reply packet with error - insufficient
resources(5) and data packets that should be taking a direct spoke-spoke
tunnel are taking the spoke-hub-spoke path.
```

Conditions: This symptom has been observed in a DMVPN Phase 3 Network when building or refreshing a spoke-spoke tunnel.

Workaround: See the Further Problem Description for how to manually see and clear the problem. The fix for CSCsd74859 "DMVPN Phase 3: Network NHRP mappings are not refreshed when being used" will help reduce the occurrence.

Further Problem Description: Use the **show ip nhrp** command to look for NHRP mapping entries that are covered by an NHRP network mapping entry in the table.

Example:

Network mapping:

```
192.168.13.0/24 via 10.0.0.13, Tunnel0 created 00:02:51, expire 00:07:08
  Type: dynamic, Flags: router nat
  NBMA address: 172.16.3.1
```

Incomplete mapping covered by above network mapping

```
192.168.13.70/32, Tunnel0 created 00:02:51, expire 00:00:13
  Type: incomplete, Flags: negative
  Cache hits: 61
```

```
192.168.13.72/32, Tunnel0 created 00:02:51, expire 00:00:13
  Type: incomplete, Flags: negative
  Cache hits: 16
```

If this example indicates the symptom is present. Clearing the incomplete mappings clears the symptom, but it can easily come back.

Example:

```
clear ip nhrp 192.168.13.70
```

Miscellaneous

- 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.

- 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.

- CSCek48151

Symptoms: When Forced target is used for Active probing, then probing may not occur in certain conditions.

Example:

```
Prefix: 10.1.1.0/24
Forced Target: 10.2.2.2
Routes on BR:
No route for 10.2.2.0/24
```

Route for 10.1.1.0/24 exists

Conditions: This symptom has been observed when Forced target is used for Active probing.

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.

- 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.

- CSCsb76992

Symptoms: DTMF digit collection will not work when using the `clid_authen_collect` tcl script with SIP. The DMTF collection does not work when used with delayed media INVITEs, which is the SIP gateway receiving an INVITE without SDP.

Conditions: The use of delayed media INVITEs with the `clid_authen_collect` tcl script will prevent the SIP gateway from collecting DTMF digits from the user.

Workaround: If possible, do not use delayed media INVITEs with the `clid_authen_collect` tcl script.

- CSCsc49798

Symptoms: The **show policy-map interface** command does not display the output as expected. The set precedence or the DSCP value configured under the **policy map** command does not get displayed under the QoS Set header but instead gets displayed at the beginning of the output. The **show policy-map** command does not display these set configurations at all.

Condition: This symptom has been seen on a Cisco 7200 router loaded with Cisco IOS interim Release 12.4(5.7) and QoS configured.

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.

- 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.

- 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.

- 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.

- CSCsd46413

Symptoms: Long configuration times are seen for very large QoS configurations (at or near 40k unique policy-map instances) for ATM PVC with policy-map per PVC.

Conditions: This symptom has been observed with very large QoS configurations and Cisco IOS Release 12.0S, Release 12.2SB, or Release 12.4T.

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.

- 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.

- CSCsd81183

Symptoms: Mallocfail error messages and tracebacks are seen on the Cisco 1802W router due to normal particle pool memory leaks.

Conditions: This symptom has been seen on a Cisco 1802W router that is running Cisco IOS Release 12.4(6)T with the **qos pre-classify** command enabled under the virtual tunnel interface.

Workaround: Disable the HW encryption, or disable the **qos pre-classify** command.

- 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.

- 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>

- CSCse20147

Symptoms: After the upgrade to Cisco IOS Release 12.3(11)YW1 and Release 12.3(11)YW3 software, huge amount of latency occurs in the data-traffic. The **show pxf cpu queue sw1** command shows that the main XFL data queues back up and the slow de-queue of the queued-up data is the cause for the latency.

Conditions: This symptom has been observed on RPM-XF cards running in the low-speed (XFL) mode and occurs after a card is upgraded to a new image. It was first observed after upgrade to YW1 image.

Workaround: Reload the PXF or reload the card.

- 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.

- 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.

- 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_elt1_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.

- CSCse58234

Symptoms: A router is crashing due to bad chunk reference count.

Conditions: This occurs on Cisco 7200 routers running Cisco IOS Release 12.4(6)T2 configured for H.323 voice services.

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>

- CSCse69102

Symptoms: Spurious memory access is made at `ike_profile_remove`.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS 12.4(6)T3, when there is at least one ike or ipsec sa and the profile is removed using the CLI with `debug crypto isakmp` turned on.

Workaround: Turn off `crypto isakmp` debugs or clear all of the crypto sessions and then remove the `isakmp` profile.

- CSCse75492

Symptoms: A router may crash due to fixing the memory leak problem in “SSS Manager.”

Conditions: This issue is observed in an LAC router.

Workaround: There is no workaround.

- 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 12.4Mainline and 12.4T release

Workaround: None

- CSCse89402

Symptoms: The CPU stack frame can 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 with the **no network-clock participate** command.

Workaround: Use the VWIC in the **network-clock participate** command 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.

- CSCsf02427

Symptoms: The PXF chip on the RPM-XF frontcard will reload continuously and the chip never becomes active. All the layer 3 protocols are down and the traffic doesn't pass through. The RPM_XF card is active but doesn't forward any traffic.

Conditions: The above situation can happen if the PXF has a hardware issue and is reloading continuously or if the software error recurs continuously, the card will be unusable.

The card will not be useful if the problem happens in datapath segmentation and reassembly chipset.

Workaround: Once the above condition is detected, the card has to be reloaded manually. In case of a redundancy setup, the standby card will takeover.

In a single card scenario, the card has to be replaced depending on the severity of the device errors.

- 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 may be a platform and software independent issue.

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>

- CSCsf07783

Symptoms: "No more IPHC-Ids" traceback is observed while doing PXF micro-code reloads. In addition, some interfaces did not get IPHC enabled on them, while others used up more than their fair share of IPHC-Ids.

Conditions: This symptom has been observed with large configurations, with over 150 interfaces enabled with IPHC and using the **micro reload pxf** command.

Workaround: Reload the card.

- CSCsf09266

Symptoms: EasyVPN negotiation fails when using EasyVPN with VTI. A %CRYPTO-6-IKMP_MODE_FAILURE will be printed to the console.

Conditions: This symptom has been observed when using EasyVPN with VTI.

Workaround: Remove VTI from the EasyVPN configuration

- CSCsf98381

Symptoms: Card crash and memory corruption messages have been observed.

Conditions: This symptom has been observed when DPC feature is enabled and when any of the datapath devices failed in RPM-XF card

Workaround: Disable the dpc device failure log and dump feature using the **hw-module rpm check datapath info-file off** command.

TCP/IP Host-Mode Services

- CSCsd74139

Symptoms: HTTP errors occur while accessing a Win2003 Web Server.

Conditions: This symptom has been observed with a Cisco IOS Voice gateway running Cisco IOS Release 12.4(6)T accessing a Win2003 HTTP web server under heavy load. Cisco IOS Voice has **ip http client connection persistent** disabled.

Workaround: There are two possible workarounds:

1. Switch to a Win2000 HTTP web server.
2. On a Win2003 server, set "TcpTimedWaitDelay" to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

Wide-Area Networking

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(6)T3

Cisco IOS Release 12.4(6)T3 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T3 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCek32177

Symptoms: The TACACS+ AV addr=255.255.255.254 will not be processed correctly with Cisco IOS interim Release 12.4(5.8)T or later.

Conditions: The symptom has been seen in testing Tacacs+ while the same scenario works fine with Radius.

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.

- 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.

- 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.

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.

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.

- 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.

- 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.
- 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.
- 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.

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

- 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.

- CSCek28887

Symptoms: The **log** action keyword is displayed incorrectly in the **show policy-map [type type] control-plane [host | transit | cef-exception | all]** output

Conditions: This symptom has been seen in Cisco IOS Release 12.4(6)T.

Workaround: There is no workaround.

Further Problem Description: The problem happens when the **log** action keyword is configured for control-plane policies. The **show policy-map [type type] control-plane [host | transit | cef-exception | all]** output shows the keyword in the wrong place.

For example, when log is configured in class-default for a policy-map LA attached to the control-plane host interface, the **show policy-map type logging control-plane all** shows this output:

```
Router#show policy-map type logging control-plane all
log <===== Wrong place
Control Plane Host
```

```
Service-policy logging input: LA
```

```
Class-map: LA (match-all)
  29 packets, 1740 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:  packets permitted
```

```
Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

The following example shows log configured for a policy-map LL attached to the control-plane cef-exception interface. Policy-map LA is still attached to the control-plane host interface but with no log action configured.

```
Router#show policy-map type logging control-plane all
```

```
Control Plane Host
```

```
Service-policy logging input: LA
```

```
Class-map: LA (match-all)
  29 packets, 1740 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:  packets permitted
```

```
Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

```
log <=====Wrong place
```

```
Control Plane Cef-exception
```

```
Service-policy logging input: LL
```

```
Class-map: LL (match-all)
  486 packets, 29160 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:  packets permitted
```

```
Class-map: class-default (match-any)
  3628 packets, 233804 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

From the display, it appears as though the log is configured for policy-map LA but it is actually configured for policy-map LL.

- 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.

- CSCek41147

Symptoms: RFC2833 is not working between Cisco CallManager Express (CME) and a Cisco AS5850 gateway in a SIP trunk service.

Conditions: This symptom has been observed on a Cisco 2800 Series Integrated Services Routers (ISR) running Cisco IOS Release 12.4(4)T2 configured for CME SIP trunking. The VoIP dial-peer has the **dtmf-relay rtp-nte** command configured.

Workaround: The only workaround is to have the Cisco AS5850 gateway configured for RFC2833 if that is possible in the network. As this change will effect live deployment, it may not be possible, in which there is no workaround.

Further Problem Description: CME is not offering RFC2833 DTMF relay capability when VoIP dial-peer has the RFC2833 DTMF relay configured.

- 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.

- CSCsa43170

Symptoms: A Cisco 2600XM series router may unexpectedly restart while handling a bus error. The original bus error was going to result in an unexpected restart. However the data normally saved after such an event may not be completely saved due to the second unexpected restart.

Conditions: This symptom affects Cisco IOS software after Cisco IOS Interim Release 12.3(10.3)T2 only on the Cisco 2600XM series of routers.

Workaround: There is no workaround.

- CSCsa45270

Symptoms: **Show policy interface Multilink no:** command shows a discrepancy in total transmitted + random drop + tail drop, the number shown to be received on the remote end, and the number of input packets.

Conditions: Data is sent to cause congestion such that there are random and tail drops.

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.

- 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.

- 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.

- 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.

- 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.

- 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 not 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.

- 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.

- 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.

- 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.

- 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 recommend 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.

- 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

- 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.

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.

- 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.

- 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.

- 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.

- 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(6)T2

Cisco IOS Release 12.4(6)T2 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T2 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCse09204

Symptoms: When upgrading from Cisco IOS Release 12.4(2)T or Cisco IOS Release 12.4(4)T, the IP SLAs echo operation configuration is lost. This defect is logged because the router (while coming up after reload) does not understand the use of "Dialer" in the *interface-name* argument of the **source-interface interface-name** command as shown in this example:

```
DRAM configuration is 64 bits wide with parity enabled.
```

```
239K bytes of non-volatile configuration memory.
```

```
250368K bytes of ATA CompactFlash (Read/Write)
```

```
type echo protocol ipIcmpEcho 10.0.0.1 source-interface Dialer1
```

```
% Invalid input detected at '^' marker.
```

```
timeout 1000
```

```
% Invalid input detected at '^' marker.
```

```
frequency 3
^
% Invalid input detected at '^' marker.
%Entry not configured
```

This symptom is related to CSCsc24145.

Conditions: This symptom has been observed on routers having the IP SLA echo operation configured with the **ip sla monitor** command, when these operations specify the Dialer as the source-interface, and when the router is being upgraded to Cisco IOS Release 12.4(4)T or later version.

Workaround: Reconfigure new operations with the new release after upgrading.

Miscellaneous

- CSCsd58630

Symptoms: The **local-address** command under the **crypto isakmp profile** global configuration does not work in Cisco IOS Release 12.4(6)T and later. The command also does not show up in the running configuration after the command is entered.

Conditions: This symptom has been observed on a Cisco router configured with IP Security (IPSec) running Cisco IOS Release 12.4(6)T and later.

Workaround: There is no workaround.

- CSCse20809

Symptoms: IKE SA processing stops at CONF_XAUTH state although the extended authentication (Xauth) username and password are configured on EzVPN Remote correctly.

Conditions: This symptom has been observed when load balancing is configured on a Cisco VPN 3000 Series Concentrator.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(6)T1

Cisco IOS Release 12.4(6)T1 is a rebuild release for Cisco IOS Release 12.4(6)T. The caveats in this section are resolved in Cisco IOS Release 12.4(6)T1 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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.

- 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 than 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.

- 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.

Interfaces and Bridging

- CSCej77191

Symptoms: Accessing some web pages results in the router appearing to hang. No IP traffic goes to or from the router. None of the lights flash. The console continuously prints the following message:

```
%SYS-2-NOTQ: unqueue didn't find 0 in queue 831A65B4
-Process= "<interrupt level>", ip1= 2
-Traceback= 0x807CBCBC 0x8008FBD8 0x806D1EB4 0x806D2020 0x8037C200 0x80135030
```

```
0x80129B34 0x8012C344 0x8012ED68 0x8034B0A4 0x800D3014 0x800D3014 0x8034B164
0x807F0654 0x807F0590 0x807ED9D4
```

The router must be power cycled to recover.

Conditions: This symptom has been observed on Cisco IOS Release 12.4T and Release 12.4(4)T when Dynamic Multipoint VPNs (DMVPN) are being used.

Workaround: Disable bridging.

- CSCsc64115

Symptom: When changing the encapsulation and exiting configuration mode on a serial interface on a Cisco 7500 router from HDLC to either PPP or Frame- Relay, the router may experience a cBus complex restart.

Conditions: This symptom has been observed in Cisco 7xxx routers using Cisco IOS Release 12.3(17).

Workaround: Manually configure an MTU value to set the maximum datagram size to what is required. However, this may affect routing protocols that require matching MTU values.

IP Routing Protocols

- CSCej70091

Symptoms: Sending a ping to the router interface does not get an answer and results in traceback.

Conditions: This symptom has been observed when FPM service policy is configured on the interface.

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.

- CSCek16041

Symptoms: A Cisco 870 router does not offer the *vrf* keyword during configuration of the **router ospf** command:

```
router(config)#router ospf ?
<1-65535> Process ID

router(config)#
```

Conditions: The symptom has been observed in Cisco IOS Interim Release 12.4(5.8)T. Only the Cisco IOS Release 12.4T train is affected. The symptom is triggered by port of CSCsb73882 in Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCsc33408

Symptoms: The router reloads unexpectedly when unconfiguring the static route.

Conditions: Remove the static route which was configured and then unconfigured from the BGP and IPv4 multicast address-family. The crash has been observed when the static route was unconfigured after clearing the bgp routes.

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.

- CSCsc70155

Symptoms: A Telnet session from a TCP host to an X.25 client may fail when the protocol translator is configured in between.

Conditions: This symptom has been observed in Cisco IOS interim Release 12.4(5.8)T.

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.

- 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
```

- 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 = 0xFFFFFFFF Process= "NHRP",
ipl= 0, pid= YYY
```

Conditions: This symptom is observed in a DMVPN environment.

Workaround: There is no workaround.

Miscellaneous

- 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.

- 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>

- CSCek27437

Symptoms: An SNMP request to delete a switch connection (setting cwaChanRowStatus to 6 [destroy]) deletes both the Swconn part and the PVC part.

Conditions: This symptom has been observed under normal conditions using SNMP to manage connections on RPM.

Workaround: There is no workaround.

- CSCek29605

Symptoms: SIP phones do not receive MWI even though a message is left for a SIP phone user.

Conditions: This symptom has been observed with SIP phones on CME and when CUE has voicemail.

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.

- CSCek30276

Symptoms: A ping fails with port adapters (PA) inserted into a C7200-I/O Jacket Card with reformation images.

Conditions: This symptom only happens with reformation images and not with classic images.

Workaround: Use a classic image or use the PA in any other slot other than ESCORT.

- 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.

- CSCek32263

Symptoms: The Parallel eXpress Forwarding (PXF) on RPM-XF card reloads and generates a log and a crashinfo file.

Conditions: Bit errors in PXF IRAM can occur, though they are extremely rare. The Bit error in PXF Instruction RAM can cause other issues, like invalid register contents, which could result in other PXF exceptions causing the reload.

Workaround: There is no workaround. The PXF crash process will reload PXF IRAM. All layer 3 connectivity comes up automatically after the PXF reloads.

- 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.

- CSCek35105

Symptoms: When the policy-map class bandwidth is modified, it fails for the multilink interface.

Conditions: This symptom has been observed with the output of the policy map attached to multilink and when changing the bandwidth allocation for a class.

Workaround: Use the **shutdown** command and then the **no shutdown** command on the switch subinterface.

- CSCek37351

Symptoms: When a caller attempts to call a SCCP phone that has Call Forward All enabled, the forwarding does not occur. The caller hears silence.

Conditions: The called party must be a SCCP phone with Call Forward All enabled.

Workaround: There is no workaround.

- CSCek38939

Symptoms: The input error counter may not be incremented for packet errors such as runs, 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.

- CSCek39078

Symptoms: "show policy-map int sw1.xx" command output is jumbled and information pertaining to a class is not fully displayed under the correct class.

Condition: With service policy-map attached to PVC execute "show policy-map int sw1.xx" command and the RPMXF card is configured as XFL. The command "atm sar-based-cbwfq" when configured on the SW1 interface will make the card to work as XFL.

Work-around: There is no workaround.

- CSCin98630

Symptoms: When an InARP request is received on an AAL5SNAP PVC, the router does not respond with an InARP reply.

Conditions: This symptom has been observed when the source address contained in InARP request is not in the subnet of the sub-interface on which PVC is configured.

Workaround: There is no workaround.

- 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.

- 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.

- 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 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: 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

- 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.

- 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.

- CSCsc31776

Symptoms: The router reloads when 3000 create requests are sent.

Conditions: The symptom has been observed when the router is running Cisco IOS GGSN Release 5.0 and 6.0 and the following conditions occur:

1. The **debug gprs gtp messages** command is turned on.
2. External DHCP IP address assignment is configured.
3. VRF is configured on the APN but not on the DHCP server.

Workaround: There is no workaround.

- 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.

- 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.

- CSCsc46528

Symptoms: ccmeEphoneActTable from CISCO-CCME-MIB provides inconsistent results.

Conditions: This symptom has been observed when a partial SNMP GET is issued on selected columns from ccmeEphoneActTable.

Workaround: Perform a complete SNMP GET instead of a few entries on ccmeEphoneActTable.

- 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.

- 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.

- 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.
- 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.
- 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.
- CSCsd69754
Symptoms: Traffic through an IPsec VPN connection does not leave the router.
Conditions: This symptom has been observed when the interface where the **crypto map** command is applied (the interface that will be the source address of the encrypted packet) is configured as a security zone-member.
Workaround: Remove the **zone-member security zone_name** command from the crypto outside interface. This will prevent the application of the Zone Firewall policy on clear-text traffic from the problem interface and other firewall security zones.
- 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.
- CSCsc80668
Symptoms: The Cisco IOS has the capability to implement HSP feature but the MIB support is incomplete. HSRP-related MIBs have not been implemented in the Cisco 800 series platforms.
Conditions: This symptom has been observed on Cisco 800 series routers.
Workaround: There is no workaround.
- 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.

- CSCsc97545

Symptoms: On a Dynamic IPsec VTI, when a packet is greater than twice the IP MTU (i.e., needing more than 2 fragments), the first fragment is transmitted but not the additional fragments.

From the **show ip traffic** command:

- The "Fragments" counter is incremented by two.
- The "Couldn't fragment" counter is incremented by one.

Conditions: This symptom has been observed when an IP packet needs more than two fragments on a router serving as an IPsec Gateway using Dynamic IPsec VTI. It is only seen when Cisco Express Forwarding (CEF) is turned on.

Workaround: There is no workaround.

- CSCsd02098

Symptoms: There is no voice path and packets are not encrypted or decrypted.

Conditions: This symptom has been observed when a call is made as an SRTP call.

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.

- CSCsd08862

Symptoms: A router may crash because of a bus error when you enter the **show interface** command or another command that displays the virtual-access information for a virtual-access interface or subinterface.

Conditions: This symptom is observed while a session that is associated with the virtual-access interface or subinterface is being cleared.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsd20136

Symptoms: Bidirectional Forwarding Detection (BFD) support was added for the Cisco 7200 and Cisco 7301 platforms in Cisco IOS Release 12.4(4)T. Some interface level BFD commands are not configurable which may prevent the full BFD feature from working.

Conditions: This symptom is seen with all feature set images of Cisco 7301 and Cisco 7200 of Cisco IOS Release 12.4(4)T and Cisco IOS Release 12.4(4)T1 except Cisco 7200 with GGSN feature set images of same versions.

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.

- 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>

- 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.

- 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.

- CSCsd69754

Symptoms: Traffic through an IPsec VPN connection does not leave the router.

Conditions: This symptom has been observed when the interface where the **crypto map** command is applied (the interface that will be the source address of the encrypted packet) is configured as a security zone-member.

Workaround: Remove the **zone-member security zone_name** command from the crypto outside interface. This will prevent the application of the Zone Firewall policy on clear-text traffic from the problem interface and other firewall security zones.

- CSCsd76813

Symptoms: On a Cisco RPM-XF Router, policing succeeds only on the last interface when the same policy-map is applied to several interfaces.

Conditions: This symptom has been observed when the same policy map is applied to several interfaces.

Workaround: Create several policy-maps with different names and apply them to the interfaces instead of applying the policy-map with the same name to all interfaces. It is also observed that the condition is rectified after some time. This time cannot be estimated. The police parameters for this situation are not exactly understood.

- 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.

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.

- 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.

- 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.

- CSCsd71360

Symptoms: PPP Multilink fragment loss occurs as the result of premature lost fragment timeouts. This can be seen in the lost fragment count in the output of the **show ppp multilink** command, as well as debug traces produced by the **debug ppp multilink events** command.

Conditions: This symptom has been observed with Cisco IOS Release 12.2(28)SB and Release 12.4(6)T, but not with Cisco IOS Release 12.2(27)SBC2 or Release 12.4(4)T

Workaround: Configure the **ppp timeout multilink lost-fragment 1** command under the Multilink interface or the Virtual-Template interface corresponding to the multilink bundle.

Resolved Caveats—Cisco IOS Release 12.4(6)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(6)T. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(6)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCej47271

Symptoms: AAA Authentication is bypassed when logging into the router a second time. After loading the image and configuring the **aaa authentication login myown local** command, a prompt for the login and password occurs. After logging out and logging back for a second time, the system goes to the console without prompting for a login and password.

Conditions: This symptom has been observed on a router running Cisco IOS interim Release 12.4(3.9)PI3d and performing these steps:

1. Configure the **aaa authentication login** command.
2. Log into the router.
3. Exit.
4. Log into router again.

Workaround: There is no workaround.

- CSCsc24145

Symptoms: When upgrading from an image running CLI phase I or II (**ip sla monitor**) to an image running CLI Phase III (**ip sla** without *monitor* keyword), the IP SLAs configuration is lost.

Conditions: This symptom has been observed on routers having **ip sla monitor** configured and upgrading to CLI Phase III (i.e., Cisco IOS Release 12.4(4)T). This does not impact a old **rtr** CLI.

Workaround: There are two workarounds:

- Reconfigure new operations with the new release, or
- Save the old configuration and convert it to a new configuration using a search-and-replace tool offline before upgrading.

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.

- CSCsb01490

Symptoms: When general Bidirectional Forwarding Detection (BFD) functionality is enabled and when Border Gateway Protocol (BGP) is configured without BFD functionality, BFD sessions may be started with the BGP neighbors. This is not proper behavior: BFD sessions should not be started when BGP is configured without BFD functionality.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

Miscellaneous

- 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>

- CSCej87060

Symptoms: GDOI operation with AES encryption is not operational. In some cases, using GDOI with AES as the encryption transform causes the router to crash.

Conditions: This symptom has been observed when AES is configured to be used in the transform-set applied to the crypto gdoi map (via the profile keyword).

Workaround: Use 3DEs in the transform.

Further Problem Description: A crash only occurs with HSP encryption engines.

- 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>.

- CSCsb86406

Symptoms: A router crashes, Security Device Manager (SDM) and/or IPSMC are unable to view signatures that have been loaded by the Customer Information Control System (CICS), and CICS is unable to view events from Cisco IOS IPS.

Conditions: These symptoms are observed after signatures are loaded via the CICS. The symptom occurs because of a version conflict between Cisco IOS IPS and CICS.

Workaround: Disable the router as a CICS and Cisco IOS IPS device.

Further Problem Description: The **debug ip ips idconf** command can help to resolve issues between CICS and Cisco IOS IPS.

- CSCsc17504

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 interim Release 12.4(3.9)T1 or a later release with a Cisco IOS firewall during session inspection under certain timing conditions.

Workaround: There is no workaround.

- CSCsc59881

Symptoms: Call forward busy to Unity gets the subscriber standard greeting instead of the busy greeting.

Condition: This symptom has been observed when Unity integrates with CME 3.4.

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.

- CSCsd28570

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 **tcclsh** command.

Workaround: This advisory with appropriate workarounds is posted at <http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

Further Problem Description: This particular vulnerability only affected Cisco IOS versions 12.3(4)T trains and onwards. (12.3 Mainline is not affected)

Please refer to the Advisories "Software Versions and Fixes" table for the first fixed release of Cisco IOS software.

Resolved Caveats—Cisco IOS Release 12.4(4)T8

Cisco IOS Release 12.4(4)T8 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T8 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

Basic System Services

- 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

Symptoms: EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

Conditions: This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGp session on a CE router. This occurs typically in the following inter-autonomous system scenario:

ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2

Workaround: Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
  address-family ipv4 vrf one
  neighbor 1.0.0.1 remote-as 100
  neighbor 1.0.0.1 activate
  neighbor 1.0.0.1 route-map FILTER in
  exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
  set extcomm-list 100 delete
!
```

- 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>

- CSCei93768

Symptoms: A Cisco router that is configured for BGP may crash and generate the following error messages:

(Note that the hex values of tracebacks and other parameters that are part of the error messages will vary with different occurrences of the symptom.)

```
%SYS-2-NOTQ: unqueue didn't find 4552953C in queue 454BE738
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC
40C3BA10 40C3CCE0
%SYS-2-NOTQ: unqueue didn't find 455294EC in queue 454BE690
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC
40C3BA10 40C3CCE0CMD: 'end'
```

```
%SYS-5-CONFIG_I: Configured from console by console
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header,
chunk 45519C14 data 4552953C chunkmagic 15A3C78B chunk_freemagic 0
-Process= "Check heaps", ipl= 0, pid= 6
-Traceback= 4063C5FC 4063C788 4065A9D0
chunk_diagnose, code = 2
chunk name is IP RDB Chunk
```

```
current chunk header = 0x0x4552952C
data check, ptr = 0x0x4552953C
```

```
next chunk header = 0x0x4552957C
data check, ptr = 0x0x4552958C
```

```
previous chunk header = 0x0x455294DC
data check, ptr = 0x0x455294EC
```

Conditions: This symptom is observed mostly with configuration changes that involve the **bgp dmzlink-bw** command for a BGP IPv4 address family, but in very rare cases, the symptom may also occur in other situations.

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.

- 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.

Miscellaneous

- CSCds25257

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

Conditions: This symptom is observed in the following topology:

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

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

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

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

- 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>.

- CSCej42879

Symptoms: A traceback may be generated when packets are transmitted over a basic IPSec connection between two peers in transmission mode and tunnel mode using multilink interfaces.

Conditions: This symptom is observed on a Cisco 3845 that runs Cisco IOS Release 12.4(5). The symptom may also affect other releases.

Workaround: There is no workaround.

- CSCsd27617

Symptoms: IKE negotiation fails with a wrong group preshared key.

Conditions: This symptom is observed on a Cisco router that has an eight character key such as "cisco123" that is defined under the EzVPN group configuration and occurs after you have entered the **password encryption aes** command.

Workaround: To prevent the symptom from occurring, do not use an eight character key under the EzVPN group. After the symptom has occurred, re-enter the group and key.

- 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.

- CSCsd78657

Symptoms: A router crashes when trying to bring up 2000 virtual tunnel interface (VTI) tunnels on the hub, dynamic VTI side. No traffic was present when tunnels were coming up.

Conditions: This symptom is observed when trying to bring up 2000 VTI tunnels on dynamic VTI side of the hub.

Workaround: Avoid bringing a large number of tunnels simultaneously.

- 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>.

- 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.

- **CSCse04136**

Symptoms: A router crashes with traceback.

Conditions: This symptom occurs when using a Cisco 7200 router that is sending traffic using IXIA after applying crypto map feature.

Workaround: There is no workaround.

Further Problem Description: The crash occurs when testing TED feature in Cisco 7200 routers. While sending packet to initiate IPSec tunnel, the router crashes with traceback.

- **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_ps63_50_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/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

- 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.

- 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>.

- 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>

- CSCsf95938

Symptoms: A memory leak occurs in the middle buffers after all onboard DSPRM pools are depleted.

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

Workaround: There is no workaround.

- 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.

- CSCsg10134

Symptoms: A router crashes when PPPoEoA sessions are torn down.

Conditions: This symptom is observed when the maximum number of class-map instances are configured on the router.

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.

- 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.

- CSCsg83326

Symptoms: IPSec does not function when IPv6 is enabled, preventing all crypto-related functions from properly operating.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4T and that has IPv6 enabled.

Workaround: There is no workaround.

- 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.

Workaround: Configure reverse SSH by entering the **ip ssh port portnum rotary group** 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-ROUTE LIMIT (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.

- CSCsh50275

Symptoms: In a DMVPN setup with spoke having overlapping ISAKMP profiles and DPD enabled, IKE quick mode fails due to ISAKMP profile mismatch. After IKE SA expiry, the IKE SA rekey triggered by ISAKMP keepalives does not use any ISAKMP profile while initiating the SA. With overlapping ISAKMP profiles present, the IKE SA might end up attaching to the incorrect ISAKMP profile instead of the one configured on the corresponding tunnel interface and the one used by original IKE SA, subsequently causing the quick mode to fail due to profile mismatch. The only way to bring them out from that stage is by clearing Phase 1 SA.

Conditions: This symptom occurs during DMVPN testing.

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>.

- CSCsi09530

Symptoms: If the **authenticate register** command is configured under the **voice register global** command, CME SIP failed to register.

Conditions: The **authenticate register** command is configured under the **voice register global** command when CME is acting as a registrar.

Workaround: Disable the **authenticate register** command under the **voice register global** command.

Further Problem Description: In registrar functionality, CME challenges an inbound register request with a 401 response. If the **authenticate register** command is configured under the **voice register global** command, the Registering Endpoint then ends a Register Request with Credentials. The Gateway Stack is not processing this request and is dropping it.

- 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>

- CSCsi80749

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>

- 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.

- CSCsj32707

Symptoms: A “SIP UPDATE” message from a Cisco CallManager or SIP Proxy Server with a “Cseq” value of 0 may be rejected or considered invalid by A Cisco gateway.

Conditions: This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.4(9)T4 or a later release and that is connected to a SIP endpoint.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(9)T3.

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

- 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.

- 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 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(4)T7

Cisco IOS Release 12.4(4)T7 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T7 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

IBM Connectivity

- CSCsf28840

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

There are workarounds available for this vulnerability.

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

Miscellaneous

- 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>.

- CSCsc75745

Symptoms: When IKE negotiation is performed with an IKE policy with AES configured when you have hardware crypto enabled on Cisco 831 routers, that IKE policy should be ignored. Instead, if that policy is selected by the IKE peer, the router crashes.

Conditions: This symptom occurs when hardware crypto is enabled with AES enabled. Software crypto is fine.

Workaround: Either disable hardware crypto (configure “no crypto engine accelerator”), or remove the IKE policies with AES configured.

- 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>.

Resolved Caveats—Cisco IOS Release 12.4(4)T6

Cisco IOS Release 12.4(4)T6 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T6 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Miscellaneous

- CSCse92359

Symptoms: The FXS ports on a Cisco IAD2400 IAD and a Cisco VG224 gateway delivers lower than advertised idle voltage, close to -37 volts. This is observed with the **idle voltage high** command already configured under the voice port.

Conditions: This symptom has been observed on a Cisco IAD2431 IAD with an Eight FXS Analog Voice Module V2.1 and with a Cisco VG224 gateway which has an onboard FXS version 2.1.

Workaround: Use an FXS port with an earlier chip revision, such as version 1.3, and configure **alt-battery-feed feed2** command under the FXS voice ports.

- 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>.

- CSCsg50635

Symptoms: On a Cisco IAD2432 IAD when putting one of the T1 controllers into Line or Payload loopback and then trying to remove the loopback with the **no loopback** command, the T1 controller loopback is not really removed even though a **show controller T1** command indicates it has been removed.

Conditions: This symptom has been observed when putting T1 controllers into Line or Payload loopback and then the **no loopback** command is issued under the T1 controller.

Workaround: Reload the Cisco IAD2432 IAD.

Further Problem Description: An indication of the loop is seen in the T1 controller. In this example, a loopback payload was applied:

```
Router(config-controller)#do show controller t1
T1 1/0 is down. (Payload Looped)
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  RX level = 0dB
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (150 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    1 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

When the **no loopback** command is applied, it appears that the loopback has been removed as in this example. However, it has not really been removed.

```
Router#show controller t1
T1 1/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  RX level = 0dB
```

```

Framing is ESF, Line Code is B8ZS, Clock Source is Line.
Data in current interval (305 seconds elapsed):
  0 Line Code Violations, 3 Path Code Violations
  10 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 1 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs

```

Resolved Caveats—Cisco IOS Release 12.4(4)T5

Cisco IOS Release 12.4(4)T5 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T5 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

Basic System Services

- 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 sent and when an AAA server is slow or unreachable.

Workaround: There is no workaround.

- CSCir00074

Symptoms: Router crashes.

Conditions: This symptom has been observed when `casnDisconnect` is set to true for pppoe session.

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 an interface number that is equal to or greater than 10.

IP Routing Protocols

- CSCek30198

Symptoms: When nexthops are modified or deleted, the nexthop tracking information doesn't get updated properly at the required time.

Conditions: This symptom has been observed when nexthops are modified or deleted.

Workaround: There is no workaround but to wait 10 minutes for the update to occur.

- CSCek42700

Symptoms: A network and host-based configuration download over serial HDLC with an IP address obtained via SLARP fails.

Conditions: This symptom has been observed with a router that has no startup- configuration (after using the **write erase** command) but is staged for autoinstall over a serial link. An IP address is obtained, but the download fails with the following error message:

```
%Error opening tftp://255.255.255.255/network-config (Socket error)
%Error opening tftp://255.255.255.255/cisconet.cfg (Socket error)
```

Without this feature, router deployment with automatic configuration download at remote sites over serial interface is not possible.

Workaround: Use another method of autoinstall if possible, or pre- configure the router before deployment.

- 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.

- 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.

- 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 (i.e. if they enter on one interface and only exit the box through another interface), or if they do not need to be duplicated to a tunnel interface running GRE over IPv6 (i.e. tunnel mode GRE ipv4 does not have this problem).

Miscellaneous

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsd15968

Symptoms: MGCP seems to be sourcing media from a different interface than what is configured under the **mgcp bind media source-interface xxx** 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 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.

- 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.

- 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.

- 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>

- 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.

- 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_dsprn_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>

- 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.

- 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-snmvp3.shtml>

- CSCsf09266

Symptoms: EasyVPN negotiation fails when using EasyVPN with VTI. A %CRYPTO-6-IKMP_MODE_FAILURE will be printed to the console.

Conditions: This symptom has been observed when using EasyVPN with VTI.

Workaround: Remove VTI from the EasyVPN configuration.

- 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

- 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 such as when a PVC virtual-circuit is unconfigured.

Conditions: This symptom has been observed when configuring the **ppp multilink endpoint mac interface** command or the **ppp multilink endpoint ip a.b.c.d** command.

Workaround: Don't use these configuration commands in IOS versions 12.3, 12.4 or 12.2SB without a fix for this DDTs.

- 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.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(4)T4

Cisco IOS Release 12.4(4)T4 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T4 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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: 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.

- 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.

- CSCse09204

Symptoms: When upgrading from Cisco IOS Release 12.4(2)T or Cisco IOS Release 12.4(4)T, the IP SLAs echo operation configuration is lost. This defect is logged because the router (while coming up after reload) does not understand the use of “Dialer” in the *interface-name* argument of the **source-interface** *interface-name* command as shown in this example:

```

DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
250368K bytes of ATA CompactFlash (Read/Write)

type echo protocol ipIcmpEcho 10.0.0.1 source-interface Dialer1
                                     ^
% Invalid input detected at '^' marker.

timeout 1000
  ^
% Invalid input detected at '^' marker.

frequency 3
  ^
% Invalid input detected at '^' marker.
%Entry not configured

```

This symptom is related to CSCsc24145.

Conditions: This symptom has been observed on routers having the IP SLA echo operation configured with the **ip sla monitor** command, when these operations specify the Dialer as the source-interface, and when the router is being upgraded to Cisco IOS Release 12.4(4)T or later version.

Workaround: Reconfigure new operations with the new release after upgrading.

- 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.

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.

- 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.

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

- 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>

- CSCek38569

Symptoms: Removing an FPM filter while the traffic matching is passing through the router can cause a crash.

Conditions: This symptom is observed on a Cisco 7200 series router.

Workaround: Do not remove the filters on a policy that is attached to the interface when traffic that can hit the filter is passing through it.

- 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.

- CSCek47653

Symptoms: A Voice Gateway can crash by bus error.

Conditions: This symptom is observed on a Cisco IAD 2430 that is running Cisco IOS Release 12.3(14)T2. MGCP Visual Message Waiting Indicator (VMWI) related function.

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>.

- 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.

- 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.

- 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.

- 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 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.

- 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.

- 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.

- 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.

- 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

```

- CSCse19644

Symptoms: An LAC router experiences a memory leak problem in the “SSS Manager” process. It takes only three days to hold 70Mbytes memory.

```

----- show process memory -----

```

```

Processor Pool Total: 167111648 Used: 147071772 Free: 20039876
I/O Pool Total: 33554432 Used: 6154720 Free: 27399712

```

```

PID TTY Allocated      Freed      Holding      Getbufs      Retbufs Process
---- snip ----
 63  0 4285815808 3019982812 103438388          0          0 SSS Manager
<<<<<<<<
 64  0          0          0      12980          0          0 SSS Test
Client
 65  0          0          0       6980          0          0 SSS Feature
Mana
 66  0          0          0       6980          0          0 SSS Feature
Time

```

Conditions: This symptom is observed in an LAC router when PPPoE session is disconnected before completing to establish the L2TP session.

Workaround: There is no workaround.

- CSCse20809

Symptoms: IKE SA processing stops at CONF_XAUTH state although the extended authentication (Xauth) username and password are configured on EzVPN Remote correctly.

Conditions: This symptom has been observed when load balancing is configured on a Cisco VPN 3000 Series Concentrator.

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.

- 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.

- CSCse47912

Symptoms: An MPF enabled Cisco 7200 or 7301 router that is running Cisco IOS Release 12.3(14)YM does not generate ICMP redirect, ICMP ttl exceeded, or ICMP unreachable message with “DF set fragmentation needed” code as it should. It does generate a corresponding ICMP message sometimes but with incorrect ICMP checksum.

Conditions: This symptom is observed on a Cisco 7200 or 7301 router with MPF enabled, and it is MPF platform dependent.

Workaround: Use TCP MSS adjustment to avoid fragmentation, or turn off MPF with the **no ip mpf** command.

- CSCse75492

Symptoms: A router may crash due to fixing the memory leak problem in “SSS Manager.”

Conditions: This issue is observed in an LAC router.

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.

- 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(4)T3

Cisco IOS Release 12.4(4)T3 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T3 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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.

- 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.

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.

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.

- 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.

- 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.

- 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.

- CSCsb01490

Symptoms: When general Bidirectional Forwarding Detection (BFD) functionality is enabled and when Border Gateway Protocol (BGP) is configured without BFD functionality, BFD sessions may be started with the BGP neighbors. This is not proper behavior: BFD sessions should not be started when BGP is configured without BFD functionality.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(31)S.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsc70155

Symptoms: A Telnet session from a TCP host to an X.25 client may fail when the protocol translator is configured in between.

Conditions: This symptom has been observed in Cisco IOS interim Release 12.4 (5.8)T.

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.

- 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.

Miscellaneous

- 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. The symptom may also occur in other 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. The symptom may also occur in other releases.

Workaround 2: 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.

- 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.

- 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.

- 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>

- 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.

- CSCek38136

Symptoms: When you deploy VoIP using PVDM2 / TI-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 TI-5510 DSP modules. The symptom does not occur with TI-549 DSP modules.

Workaround: There is no workaround.

- CSCek41147

Symptoms: RFC2833 is not working between Cisco CallManager Express (CME) and a Cisco AS5850 gateway in a SIP trunk service.

Conditions: This symptom has been observed on a Cisco 2800 Series Integrated Services Routers (ISR) running Cisco IOS Release 12.4(4)T2 configured for CME SIP trunking. The VoIP dial-peer has the **dtmf-relay rtp-nte** command configured.

Workaround: The only workaround is to have the Cisco AS5850 gateway configured for RFC2833 if that is possible in the network. As this change will effect live deployment, it may not be possible, in which there is no workaround.

Further Problem Description: CME is not offering RFC2833 DTMF relay capability when VoIP dial-peer has the RFC2833 DTMF relay configured.

- 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>.

- 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.

- 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.

- 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.

- 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.

- 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.

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 occur only on a single voice port, there is another problem, not this caveat (CSCsc11833). 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: 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.

- 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.

- 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.

- 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.

- CSCsc55406

Symptoms: A memory leak occurs whenever an Embedded Event Manager (EEM) Tcl policy is run.

Conditions: The symptom has been observed when an EEM Tcl policy is run.

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 (Ecuudp) 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.

- 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.

- 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.

- 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.

- 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 not 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.

- 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.

- 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.

- 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.

- CSCsd30932

Symptoms: Issuing the **trust-point storage** command sometimes causes a crash.

Conditions: This symptom only occurs when an error occurs on a previous execution of this command. The second execution of the command results in a crash.

Workaround: If an error occurs when issuing this command, the trustpoint must be removed and re-created to avoid a crash.

- 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.

- 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.

- 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>

- 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 recommend 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.
- 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.

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.

- 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.

- 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.

- 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(4)T2

Cisco IOS Release 12.4(4)T2 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T2 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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.

- 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.

- CSCej30903

Symptoms: The router allows logging into the root (or any other configured) view without prompting for the password.

Conditions: No method list should be configured for login.

Workaround: Configure the method list for the login service.

- 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.

- 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.

- 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.

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.

- 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. However, the symptom is not platform-specific and release-specific.

Workaround: There is no workaround.

IP Routing Protocols

- 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.

- 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.

- 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.

- 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.

- 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. If this is not an option, 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.

- 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.

- CSCsc33408

Symptoms: The router reloads unexpectedly when unconfiguring the static route.

Conditions: Remove the static route which was configured and then unconfigured from the BGP and IPv4 multicast address-family. The crash has been observed when the static route was unconfigured after clearing the bgp routes.

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.

- CSCsc78813

Symptoms: While using NAT in an overlapping network configuration, the IP address inside a DNS reply payload from the nameserver is not getting translated at the NAT BOX.

Conditions: The above symptom is seen in Cisco routers that are loaded with Cisco IOS Release 12.3(18) image, configured with the **ip nat outside source** command.

Workaround: There is no workaround.

Miscellaneous

- CSCed28266

Symptoms: A Cisco gateway may unexpectedly reload because of a software-forced crash when it builds a SIP ACK(nowledge) or BYE message.

Conditions: This symptom is observed when the gateway receives a SIP response that contains a Record-Route header and a Contact header and when the length of the Contact header exceeds 128*n, in which "n" is the number of URLs in the Record-route header.

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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCej22954

Symptoms: The **show event manager history events [detailed] [maximum number]** command may crash when the history queue has looped.

Conditions: The default size of the Embedded Event Manager (EEM) history events queue is 10. If 11 events come in, then the *number* argument with a value less than 10 will cause the issue. This symptom only affects routers using the EEM and with the **show event manager history events** command using the **maximum** keyword.

Workaround: Do not use the **maximum** keyword.

- 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.

- 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.

- CSCek25330

Symptoms: Traffic does not flow in the setup on the LAC----Client connection. The Tx locks up after 5 retries during the GigEth Tx underflow.

Conditions: This symptom has been observed when bidirectional traffic is sent in a hairpinning setup.

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.

- 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.

- 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.

- 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.

- 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**.

- 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.

- 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.

- 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.

- 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 devices are configured on the FXS port but is not limited to this configuration.

This particular instance is when using MGCP controlled voice ports.

Workaround: Use H323 for signaling.

- 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
```

- 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.

- 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.

- 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.

- CSCsc16282

Symptoms: When GDOI is used in the Transport mode when using a VAM2 card, GDOI packets are corrupted which gives rise to checksum failures.

Conditions: This symptom has been observed when GDOI is used in the Transport mode with a VAM2 card.

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.

- 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.

- 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.

- CSCsc39491

Symptoms: 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.

- 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.

- 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.

- CSCsc46528

Symptoms: ccmeEphoneActTable from CISCO-CCME-MIB provides inconsistent results.

Conditions: This symptom has been observed when a partial SNMP GET is issued on selected columns from ccmeEphoneActTable.

Workaround: Perform a complete SNMP GET instead of a few entries on ccmeEphoneActTable.

- 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.

- 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.

- 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".

- CSCsc80668

Symptoms: The Cisco IOS has the capability to implement HSP feature but the MIB support is incomplete. HSRP-related MIBs have not been implemented in the Cisco 800 series platforms.

Conditions: This symptom has been observed on Cisco 800 series routers.

Workaround: There is no workaround.

- CSCsc94149

Symptoms: Cisco 876 and Cisco 877 routers fail to synchronize with third-party vendor DSLAMs.

Condition 1. The DSL line of a Cisco 876 router with the **dsl operating-mode auto** command configured fails to synchronize with a third-party vendor DSLAM and line card SU ADSL 32I (TI chipset).

Condition 2. The DSL line of Cisco 876 and Cisco 877 routers with the **dsl operating-mode auto** command configured fails to synchronize in ADSL2/2+ Rate-Adaptive mode with another third-party vendor DSLAM at and below 2000m line loop length with maximum data rates configured as 512/512 Kbps upstream and downstream.

Workaround 1. There is no workaround.

Workaround 2. For 512/512 Kbps profile, if the line operating mode is set to itu-dmt, the line trains up fine in ADSL1 mode.

- CSCsc94359

Symptoms: BGP table and CEF forwarding table have mismatched labels.

Conditions: The trigger to this symptom seems to be a BGP flap that happened between another PE and CE.

Workaround: Shut down the redundant link and use the **clear ip route vrf** command.

- CSCsc97545

Symptoms: On a Dynamic IPsec VTI, when a packet is greater than twice the IP MTU (i.e., needing more than 2 fragments), the first fragment is transmitted but not the additional fragments.

From the **show ip traffic** command:

- The "Fragments" counter is incremented by two.
- The "Couldn't fragment" counter is incremented by one.

Conditions: This symptom has been observed when an IP packet needs more than two fragments on a router serving as an IPsec Gateway using Dynamic IPsec VTI. It is only seen when Cisco Express Forwarding (CEF) is turned on.

Workaround: There is no workaround.

- CSCsd08862

Symptoms: A router may crash because of a bus error when you enter the **show interface** command or another command that displays the virtual-access information for a virtual-access interface or subinterface.

Conditions: This symptom is observed while a session that is associated with the virtual-access interface or subinterface is being cleared.

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.

- CSCsd20136

Symptoms: Bidirectional Forwarding Detection (BFD) support was added for the Cisco 7200 and Cisco 7301 platforms in Cisco IOS Release 12.4(4)T. Some interface level BFD commands are not configurable which may prevent the full BFD feature from working.

Conditions: This symptom is seen with all feature set images of Cisco 7301 and Cisco 7200 of Cisco IOS Release 12.4(4)T and Cisco IOS Release 12.4(4)T1 except Cisco 7200 with GGSN feature set images of same versions.

Workaround: There is no workaround.

- CSCsd35970

Symptoms: With IPsec Virtual Tunnel interfaces configuration, packets with df-bit set are dropped.

Conditions: To avoid fragmentation, the IP MTU on the IPsec Virtual Tunnel Interface is set to 1400. But when a packet of 1400 size is sent with DF-bit set, IPsec sends an ICMP PMTU error with MTU of 1473.

Workaround: Send packets with DF-bit clear, which may not be acceptable to the customers.

- 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>

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

- 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.

- 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.

- 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.

- 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.

- CSCsc95588

Symptoms: A Cisco router reloads when the **show log**, **show interface**, or **show caller** commands are issued.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.3(5b), but it can happen on any Cisco IOS 12.3 release. This symptom can occur when PPP sessions go down while the show output is suspended.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(4)T1

Cisco IOS Release 12.4(4)T1 is a rebuild release for Cisco IOS Release 12.4(4)T. The caveats in this section are resolved in Cisco IOS Release 12.4(4)T1 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCsc24145

Symptoms: When upgrading from an image running CLI phase I or II (**ip sla monitor**) to an image running CLI Phase III (**ip sla** without *monitor* keyword), the IP SLAs configuration is lost.

Conditions: This symptom has been observed on routers having **ip sla monitor** configured and upgrading to CLI Phase III (i.e., Cisco IOS Release 12.4(4)T). This does not impact a old **rtr** CLI.

Workaround: There are two workarounds:

1. Reconfigure new operations with the new release, or
2. Save the old configuration and convert it to a new configuration using a search-and-replace tool offline before upgrading.

Miscellaneous

- 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.

- 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.

- 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.

- 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>

- CSCej25000

Symptoms: Traceback is observed in the log after attaching service-policy on ATM interface.

Conditions: This symptom was observed on a Cisco 7200 router when NBAR was not configured, but the symptom is not platform dependent and may occur on other platforms in a similar configuration.

Workaround: There is no workaround but this traceback does not affect the configured service policy.

- 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.

- CSCej46631

Symptoms: A Cisco 1801 router might crash with a watchdog timeout after displaying some %SYS-3-CPUHOG messages pointing to the ILPM process.

Conditions: This symptom has been observed on a Cisco 1801 router running Cisco IOS Release 12.3(14)YT or 12.3(14)YT1.

Workaround: Do not disconnect PoE supply at the router connector without first switching off the AC supply to the PoE power brick. Also, do not rapidly switch on and off the PoE power supply.

- 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.

- 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 expect 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.

- 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.

- 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.

- 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. This crash may occur when the peer sends a certificate wrapped in an PKCS7 envelope and the validation fails. When the peer tries to resend the certificate the router may crash.

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.

- 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.

- CSCsb84615

Symptoms: The error message appears on a Cisco 1812 router during high traffic load.

*Sep 9 04:54:38.468: %MOTCR-3-CMD_ERR: MOTCR command returned error: (0x1048)

*Sep 9 04:54:38.468: motcr_lopri_error: unknown error 0x1048

*Sep 9 04:54:38.468: IPSECcard: an error coming back 0x1048

*Sep 9 04:54:38.688: %MOTCR-3-CMD_ERR: MOTCR command returned error: (0x1048)

*Sep 9 04:54:38.688: motcr_lopri_error: unknown error 0x1048

*Sep 9 04:54:38.688: IPSECcard: an error coming back 0x1048

*Sep 9 04:54:38.912: %MOTCR-3-CMD_ERR: MOTCR command returned error: (0x1048)

*Sep 9 04:54:38.912: motcr_lopri_error: unknown error 0x1048

*Sep 9 04:54:38.912: IPSECcard: an error coming back 0x1048

Conditions: This symptom has been observed on Cisco 180x and Cisco 181x routers with Cisco IOS Release 12.4(2)T, Release 12.4(2)T1, Release 12.4(2)YI, Release 12.4(2)YT, and Release 12.4(2)XA and with the k9 images.

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.

- 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.

- 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.

- CSCsc43461

Symptoms: A Cisco IOS router configured for IP Security (IPSec) may drop every other packet if the crypto interface has an input Access Control List (ACL) that does not explicitly permit traffic for the inner data packets, i.e., what is encapsulated inside of IPSec.

Conditions: This symptom has been observed on a Cisco IOS router running Cisco IOS interim Release 12.4(3.9)T7 or newer configured for IPSec and the crypto interface has an input ACL that does not explicitly permit traffic for the inner data packets.

Workaround: Do not configure the IPSec and explicitly allow inner data packets to be encapsulated by IPSec.

- CSCsc54426

Symptoms: Traffic from the inside subnet does not pass.

Conditions: This symptom has been observed only with EzVPN VTI and the inside subnet configured on the EzVPN profile.

Workaround: There is no workaround.

Wide-Area Networking

- 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.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(4)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(4)T. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(4)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCsb52925

Symptoms: A router crashes while running an IP SLA jitter operation.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(3.2)T when a nonexistent VRF is configured for the jitter operation.

Workaround: There is no workaround.

IP Routing Protocols

- CSCin95836

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

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

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

NHRP is not enabled by default for Cisco IOS.

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

This advisory is posted at

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

Miscellaneous

- 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>.

- CSCeh35254

Symptoms: A dynamically applied policy map may become detached from a VC.

Conditions: This symptom is observed when you change the queue depth for the VC class and apply the new configuration to the VC while a session is active.

Workaround: There is no workaround.

- CSCeh61857

Symptoms: You may not be able to configure anything under a non-DOT11 subinterface, not even the IP address.

Conditions: This symptom is observed on Cisco 870 series, Cisco 2800 series, and Cisco 3800 series, but may also affect other routers.

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 **telsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

- CSCei42520

Symptoms: When an E&M voice interface card (VIC) is installed in the High-Speed WAN Interface Card (HWIC) slot of an Integrated Services Router (ISR), the **bootup e-lead off** voice-port configuration command does not function.

Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series.

Workaround: There is no workaround.

- CSCei49156

Symptoms: An L2TP tunnel that is initiated by a client and that has a pseudowire class configuration does not function. The **pseudowire-class** command and **interface virtual-ppp** command are rejected by the router.

Conditions: This symptom is observed only on a Cisco 850 series.

Workaround: There is no workaround.

- CSCei49850

Symptoms: The **ip dhcp client update** command is not accepted on subinterfaces.

Conditions: This symptom is observed on a Cisco router when you attempt to configure Dynamic DNS.

Workaround: There is no workaround.

- CSCei58665

Symptoms: The output of the **show access-list compiled** command may show some Turbo ACLS as unsupported, causing an implicit deny of all traffic that leaves through the interface on which these ACLS are applied.

Conditions: This symptom is observed when both CBAC and TACL are enabled and when CBAC modifies TACL on non-CBAC interfaces to ensure that traffic can be returned.

Workaround: Disable TACL. If this is not an option, there is no workaround.

- CSCei71944

Symptoms: The duration of the injected tone configured in the **voice-class tone-signal** command is shorter than the configured time. The shortest tone is on usually the last tone played.

Conditions: This symptom has been observed when the **voice-class tone-signal** command is configured on the Land Mobile Radio (LMR) port.

Workaround: Configure the command for 10 ms longer than what is actually needed for the last signal.

- CSCei71950

Symptoms: During Group Domain of Interpretation (GDOI) rekeys, the following error message and traceback may be generated:

```
%SYS-3-MGDTIMER: Uninitialized timer, set_exptime, timer = 66D55618.
-Process= "Crypto IKMP", ipl= 0, pid= 175
-Traceback= 0x607656DC 0x60877F20 0x60878824 0x60878A10 0x629D2BC4 0x629D311C
0x629D32A8 0x629DB6CC 0x629DDB78
```

Conditions: This symptom is observed on a Cisco router that is configured for IPsec and multicast.

Workaround: Do not enable GDOI rekeys.

- CSCei73829

Symptoms: Cisco VPN Client 4.6.x connected to a Cisco IOS router configured as the VPN Server passes traffic correctly but after phase 2 SA rekeys, repeated phase 2 SA rekeying occurs and the Cisco VPN Client disconnects. The client log shows:

```
2007 20:18:34.732 08/06/05 Sev=Warning/2 IKE/0xE3000099
Immature Navigation Termination due to error (Navigator:195)
```

The router debug shows:

```
IPSEC(update_key_lifetimes): volume lifetime reached 0, dropping SA sibling
```

Conditions: This symptom has been observed with Cisco VPN Client 4.6.x connected to a router configured as the VPN Server and running Cisco IOS Release 12.4(2)T.

Workaround: Downgrade the router to Cisco IOS Release 12.4(3).

- CSCei76753

Symptoms: BRI backhauling does not work on Cisco 2801 routers.

Conditions: This symptom has been seen on Cisco 2801 routers with Cisco IOS interim Release 12.4(02.02)T and Cisco IOS Release 12.4(2)T1. Backhauling works perfectly with Cisco IOS interim Release 12.4(1.9).

Workaround: There is no workaround.

- CSCei78836

Symptoms: When PPPoE L2TP sessions are brought up, a “Cannot insert into AVL tree” error message is generated for each session that is brought up.

Conditions: This symptom is observed only when a policy map is applied to the virtual template interface that is used for the sessions.

Workaround: There is no workaround.

- CSCei81698

Symptoms: When Cisco CallManager Express (CME) 3.4 interworks with Cisco Unity 4.1, Unity may send a Message Waiting Indication (MWI) notification to CME for extensions that are not configured on CME.

Conditions: This symptom is observed when you configure Cisco Unity 4.1 with some mailboxes and then reset Unity. (Doing so may cause CME to crash.)

Workaround: There is no workaround.

- CSCei83122

Symptoms: Although a Flexible Packet Matching (FPM) service policy can be applied to the host and transit control-plane configuration submodes, the FPM service policy does not apply the expected policy action (for example, a drop action) to matching packets because FPM functionality is not supported in the host and transit control-plane configuration submodes.

Conditions: This symptom is observed for any FPM policy.

Workaround: Do not apply an FPM service policy to host and transit control-plane configuration submodes.

Further Problem Description: Note that an FPM service policy can be applied and does work correctly in the control-plane configuration mode.

- CSCei84687

Symptoms: When an E&M port is configured for Land Mobile Radio (LMR) signaling, VAD is disabled, and a trunk call occurs, the voice packets are sent across even though the m-lead is off.

Conditions: This symptom is observed when the **lmr m-lead audio-gate-in** command is enabled and when the m-lead is off. In this mode, the voice packets should be generated only when the m-lead is on.

Workaround: Use VAD to control voice packet generation.

Further Problem Description: Because voice packets are always generated, the voice port on the other side that is connected to a radio has the radio always keyed up.

- CSCei87058

Symptoms: UDP-based IP packets that are generated by a PE router and sent to a VRF IP address may not be forwarded.

Conditions: This symptom is observed in an MPLS VPN network.

Workaround: There is no workaround.

- CSCei90038

Symptoms: A back-to-back ping triggers an EzVPN tunnel. A ping from a traffic generator to an EzVPN inside interface triggers a tunnel, which is then successfully established. This is improper behavior.

Conditions: This symptom is observed on a Cisco 2801 that runs an interim release for Cisco IOS Release 12.4(4)T. Note that this caveat is resolved in Release 12.4(4)T.

Workaround: There is no workaround.

- CSCej00020

Symptoms: A Cisco IP Key Server crashes when you enter the **clear crypto isakmp sa** command for a Group Domain of Interpretation (GDOI).

Conditions: This symptom is observed when you enter the **clear crypto isakmp sa** command during rekeys.

Workaround: Do not enter the **clear crypto isakmp sa** command for a GDOI during rekeys.

- CSCej22099

Symptoms: A router crashes in the “qos_notify_cb_configured” function when an AAA session is brought up.

Conditions: This symptom is observed when the AAA session is used to download QoS information and attributes from a RADIUS server. The crash does not occur when there are no attributes to download.

Workaround: There is no workaround.

- CSCej24974

Symptoms: When per-session QoS is cleared, each session causes an error message, quickly causing the console to be flooded.

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

Workaround: There is no workaround.

- CSCin94359

Symptoms: An EzVPN client does not propose AES as encryption algorithm during ISAKMP negotiation, though it is supported on a router that runs Cisco IOS software.

Conditions: This symptom is observed when AES is configured on the EzVPN server side.

Workaround: There is no workaround.

- CSCin96534

Symptoms: Cisco 1800 series and Cisco 1810 series routers crash upon enabling dot1x.

Conditions: The crash has been seen only when enabling dot1x on an onboard FE interface and not on the switch ports.

Workaround: There is no workaround.

- CSCin97578

Symptoms: EzVPN traffic with a VTI configuration is not sent to the enterprise network.

Conditions: This symptom is observed in network-extension or network-plus mode when a split-tunnel policy is enforced by the server.

Workaround: Remove the split-tunnel policy from the server.

- 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.

- CSCsa90842

Symptoms: Transparent IPS and Transparent Firewall functionality is missing from certain Cisco IOS images for the Cisco 3725 and Cisco 3745 routers.

Conditions: This functionality can not be used on the following images:

- c3725-adventerprisek9-mz
- c3725-adventerprisek9_ivs-mz
- c3725-adventerprisek9_sna-mz
- c3745-adventerprisek9-mz
- c3745-adventerprisek9_ivs-mz
- c3745-adventerprisek9_sna-mz

Workaround: To use this functionality, use the following images:

- c3725-advsecurityk9-mz
- c3725-advipservicesk9-mz
- c3745-advsecurityk9-mz
- c3745-advipservicesk9-mz

- 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>.

- 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>.

- CSCsb11124

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

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

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

- CSCsb12598

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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



Note

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- 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>

- CSCsb42436

Symptoms: In a remote access IPSec scenario using EzVPN clients to connect to a Cisco IOS router, the router crashes with an address error as soon as the IPSec sa idle timer expires. It appears that the timer expires and terminates the session, which causes the error and subsequent crash.

Conditions: This symptom has been observed when the ISAKMP idle time is configured. If the ISAKMP idle time is not configured, the crash does not occur.

Workaround: Do not configure idle time for ISAKMP.

- CSCsb52697

Symptoms: E-mail messages can be sent from a third-party vendor messenger application through the invite option, but these messages escape from the firewall block rule and pass successfully.

Conditions: This symptom is observed on a Cisco router that is configured with a Cisco IOS Firewall.

Workaround: There is no workaround.

- CSCsb56224

Symptoms: A buffering problem occurs on the AUX line on the Cisco 851 and Cisco 871 routers. The last character of AT commands from router AUX line (line 1) is displayed only after the first “RETURN” character. After the second “RETURN” character, the AT command is executed by the analog modem. This behavior is causing problems with chat scripts and sending AT commands to analog modem, making dial out impossible using chat scripts. It is possible to send AT commands to the modem using reverse telnet (AUX port). After each command, the “enter” key must be pressed twice. Even entering command characters like AT, the letter A is echoed after pressing T, T is echoed after next character, and so on.

Conditions: This symptom affects the AUX functionality of the Cisco 851 and Cisco 871 routers. Dial backup and remote management are not possible in these routers.

Workaround: There is no workaround.

- CSCsb58269

Symptoms: EzVPN fails to connect to a Cisco VPN 3000 series concentrator, and an “Unknown DOI” error message is generated.

Conditions: This symptom is observed on a Cisco router that runs an interim release for Cisco IOS Release 12.4(4)T. Note that this caveat is resolved in Release 12.4(4)T.

Workaround: There is no workaround.

- CSCsb59344

Symptoms: A group member cannot rekey and fails to reregister with the Cisco IP Key Switch (KS) after the SA has expired, causing traffic to be dropped.

Conditions: This symptom is observed after the **sa ipsec** command is removed from the Cisco IP KS.

Workaround: After the **sa ipsec** command is removed from the Cisco IP KS, enter the **clear crypto gdoi** command on both the Cisco IP KS and on the group member to clear the Group Domain of Interpretation (GDOI).

- CSCsb59652

Symptoms: A running configuration that contains a service policy may not be saved into non-volatile memory.

Conditions: This symptom is observed when an input service policy is attached to a virtual-template interface that is used for IPSec tunnels.

Workaround: There is no workaround.

- CSCsb59813

Symptoms: The H323-SIP gateway rejects valid SUBSCRIBEs with a “481 Call Leg/Transaction Does Not Exist” response message. The gateway may also crash.

Conditions: This symptom has been observed after the gateway receives an INVITE with Replaces header for a call that has an active subscription, and then subsequent SUBSCRIBE requests are received for that call.

Workaround: There is no workaround.

- CSCsb66978

Symptoms: A router crashes when you delete a call that has third-party vendor debugs enabled.

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

Workaround: Do not enable the third-party vendor debugs.

- CSCsb70282
Symptoms: Wireless LAN Context Control Protocol (WLCCP) port 2887 is open on a Cisco 1812 ISR.
Conditions: This symptom is observed on a Cisco 1812 ISR that is not wireless capable.
Workaround: There is no workaround.
- CSCsb73190
Symptoms: NAT may not function with dual tunnels.
Conditions: This symptom is observed when the tunnel that came up first goes down. In this situation, NAT does not function for the remaining tunnel.
Workaround: Configure network-extension mode for one of the tunnels.
- CSCsb82158
Symptoms: Tracebacks are generated when Cisco IOS Firewall allow and deny actions for an alarm configuration are used for a third-party vendor application.
Conditions: This symptom is observed only when all of the following conditions are present:
 - Configurations are changed while sessions come up and are torn down in fast succession.
 - Scripts are used.
 - A file transfer occurs.
 Workaround: There is no workaround.
- CSCsb85920
Symptoms: The default route is added on the EzVPN server.
Conditions: When the inside interface has no IP address assigned or the cascaded ACL has the **ip any any** command, a default route gets pushed to the server which the server adds without validating.
Workaround: Ensure the inside interface has an IP address. Do not add the **ip any any** command to a cascaded network access-list.
- CSCsb85927
Symptoms: Previous routes on the EzVPN server are not deleted when the EzVPN client reconnects.
Conditions: This symptom has been observed when the old routes are not deleted when a new connection from the same peer is received. This situation happens when the session is not closed properly by the client.
Workaround: There is no workaround.
- CSCsb86406
Symptoms: A router crashes, Security Device Manager (SDM) and/or IPSMC are unable to view signatures that have been loaded by the Customer Information Control System (CICS), and CICS is unable to view events from Cisco IOS IPS.
Conditions: These symptoms are observed after signatures are loaded via the CICS. The symptom occurs because of a version conflict between Cisco IOS IPS and CICS.
Workaround: Disable the router as a CICS and Cisco IOS IPS device.
Further Problem Description: The **debug ip ips idconf** command can help to resolve issues between CICS and Cisco IOS IPS.

- CSCsb87956

Symptoms: A software loop enters the IKE_CONFIG_MODE state.

Conditions: This symptom is observed when the following events occur:

1. A user is normally connected to the IPsec gateway through a NAT-T device.
2. The physical connection goes down on the user side, the interface is shut down, and SafeNet disconnects, but the connection is still up on the IPsec gateway.
3. The physical connection goes up on the user side and a new connection is attempted before DPD causes the old connection to go down on the IPsec gateway.

Workaround: After a disconnection, wait for DPD to tear down the IPsec/ISAKMP sessions. In a production network, there is no workaround.

- CSCsb90919

Symptoms: After a user goes on-hook when a routine call is preempted by a precedence call, there is no precedence ring tone on the receiving phone. Instead a normal ring tone sounds.

Conditions: This symptom is observed when the phone is connected to a Cisco router that runs an interim release of Cisco IOS Release 12.4(4)T. Note, however, that this caveat is resolved in Release 12.4(4)T. The symptom may also occur in Release 12.4(2)T.

Workaround: There is no workaround.

- CSCsc21467

Symptoms: An EzVPN tunnel hangs in the IPSEC_ACTIVE state.

Conditions: This symptom is observed when Extended Authentication (Xauth) is configured.

Workaround: Enter the **clear crypto ipsec client ezvpn** command to reset the EzVPN client.

- 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>

Resolved Caveats—Cisco IOS Release 12.4(2)T6

Cisco IOS Release 12.4(2)T6 is a rebuild release for Cisco IOS Release 12.4(2)T. The caveats in this section are resolved in Cisco IOS Release 12.4(2)T6 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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.

- 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>.

- 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.

- CSCse85200

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

Conditions: 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.

- 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 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

Symptoms: EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

Conditions: This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGp session on a CE router. This occurs typically in the following inter-autonomous system scenario:

```
ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2
```

Workaround: Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
  address-family ipv4 vrf one
  neighbor 1.0.0.1 remote-as 100
  neighbor 1.0.0.1 activate
  neighbor 1.0.0.1 route-map FILTER in
  exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
  set extcomm-list 100 delete
!
```

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

Miscellaneous

- CSCds25257

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

Conditions: This symptom is observed in the following topology:

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

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

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

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

- CSCdz55178

Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                                0000000001111111111222222222333^
                                12345678901234567890123456789012|
                                                                |
                                                                PROBLEM
                                                                (Variable Overflowed).
```

Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- 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>.

- 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.

- 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.

- 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.

- CSCei87058

Symptoms: UDP-based IP packets that are generated by a PE router and sent to a VRF IP address may not be forwarded.

Conditions: This symptom is observed in an MPLS VPN network.

Workaround: There is no workaround.

- CSCin90682

Symptom: A Cisco IOS device configured for IKE/IPSec may reload.

Conditions: A Cisco IOS device is configured for IKE/IPsec and receives a crafted IKE packet.

Workaround: Disable IPSec.

- 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.

- 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.

- 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>.

- 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/tac1.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/iac1.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.

- 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.

- 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>

- 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/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

- 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.

- 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>.

- 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>

- 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>.

- 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.

- CSCsg10134

Symptoms: A router crashes when PPPoEoA sessions are torn down.

Conditions: This symptom is observed when the maximum number of class-map instances are configured on the router.

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 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>.

- 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.

Workaround: Configure reverse SSH by entering the **ip ssh port portnum rotary group** 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>.

- 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>.

- CSCsi09530

Symptoms: If the **authenticate register** command is configured under the **voice register global** command, CME SIP failed to registered.

Conditions: The **authenticate register** command is configured under the **voice register global** command when CME is acting as a registrar.

Workaround: Disable the **authenticate register** command under the **voice register global** command.

Further Problem Description: In registrar functionality, CME challenges an inbound register request with a 401 response. If the **authenticate register** command is configured under the **voice register global** command, the Registering Endpoint then ends a Register Request with Credentials. The Gateway Stack is not processing this request and is dropping it.

- 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>.

- CSCsi80749

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>.

- 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.

- CSCsj32707

Symptoms: A “SIP UPDATE” message from a Cisco CallManager or SIP Proxy Server with a “Cseq” value of 0 may be rejected or considered invalid by A Cisco gateway.

Conditions: This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.4(9)T4 or a later release and that is connected to a SIP endpoint.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(9)T3.

- CSCsk13976

Symptoms: A router acting as HA that is configured with PIM may crash when a state change is observed with the neighbor during the unconfiguration.

Conditions: This symptom occurs when the interfaces on HA and its neighbor are configured with sparse-dense mode [PIM]. The crash happens while doing a “writer term” during the unconfiguration phase.

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.

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

- 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: Configure “no ppp link reset.”

- 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.

- 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.

- 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(2)T5

Cisco IOS Release 12.4(2)T5 is a rebuild release for Cisco IOS Release 12.4(2)T. The caveats in this section are resolved in Cisco IOS Release 12.4(2)T5 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.
- 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.

- 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.

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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsb27969

Symptoms: The IPv6 PIM register encapsulation tunnel does not come up after a switchover. The PIM Register mechanism does not work for sources directly connected to the router.

Conditions: This symptom has only been observed when the **ipv6 pim register-source** global configuration command is configured.

Workaround: After switchover, unconfigure and re-configure the **ipv6 pim register-source** 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.

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.

- 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.

- 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.

- 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>

- 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>

- 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.

- 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.

- 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.

Conditions: 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.

- 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>.

- 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.

- 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.

- 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 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.

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 occur only on a single voice port, there is another problem, not this caveat (CSCsc11833). 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: 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
```

- 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.

- 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.

- 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.

- CSCsc55406

Symptoms: A memory leak occurs whenever an Embedded Event Manager (EEM) Tcl policy is run.

Conditions: The symptom has been observed when an EEM Tcl policy is run.

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 (Ecuudp) 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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>

- 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 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
```

- 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
```

- 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
```

- 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
```

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.

- 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.

- 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(2)T4

Cisco IOS Release 12.4(2)T4 is a rebuild release for Cisco IOS Release 12.4(2)T. The caveats in this section are resolved in Cisco IOS Release 12.4(2)T4 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

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

- 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.

- 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.

- 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.

Miscellaneous

- CSCed28266

Symptoms: A Cisco gateway may unexpectedly reload because of a software-forced crash when it builds a SIP ACK(nowledge) or BYE message.

Conditions: This symptom is observed when the gateway receives a SIP response that contains a Record-Route header and a Contact header and when the length of the Contact header exceeds $128*n$, in which "n" is the number of URLs in the Record-route header.

Workaround: There is no workaround.

- CSCeg70988

Symptoms: The DSP crashes while making fax calls.

Conditions: This symptom has been observed on ISR.

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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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).

- 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.

- CSCej87817

Symptoms: Policing is not dropping any packets after the offered/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.

- CSCsa77411

Symptoms: A crash that is related to MPLS TE bandwidth management may occur on a Cisco router which is configured for OSPF and MPLS Traffic Engineering.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCef16096 when the following conditions are present:

- The router is configured for OSPF and MPLS traffic engineering (TE).
- The interfaces, OSPF adjacencies, and TE tunnels are flapping.
- There are more than 300 OSPF interfaces (in any state, including administratively down) in the OSPF area that is configured for MPLS TE.

You can check the number of interfaces by entering the **show ip ospf** or **show ip ospf interface brief** command. Note that all interfaces that are covered by network statements are included in the command output, even those that are in the administratively down state.

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: 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.

- 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.

- 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 12.1E or 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.

- 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.

- 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.

- 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.

- 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
```

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 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.

- 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.

- CSCsc80668

Symptoms: The Cisco IOS has the capability to implement HSP feature but the MIB support is incomplete. HSRP-related MIBs have not been implemented in the Cisco 800 series platforms.

Conditions: This symptom has been observed on Cisco 800 series routers.

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.

- 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>

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

- 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.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(2)T3

Cisco IOS Release 12.4(2)T3 is a rebuild release for Cisco IOS Release 12.4(2)T. The caveats in this section are resolved in Cisco IOS Release 12.4(2)T3 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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.

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.

- 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.

- 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.

- CSCin95836

Symptoms: Any or all of the following symptoms may occur on a platform that receives an invalid packet and replies with an error message to the sender along with part of the original packet:

- A large size memory allocation may occur and a traceback may be generated.
- Memory alignment errors may occur.
- A bad address access may occur.
- The platform may crash.

Conditions: This symptom is observed on a Cisco platform that is configured for NHRP.

Workaround: There is no workaround.

- 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

- 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.

- CSCeh40161

Symptoms: When a branch router attempts to access the Internet via HTTP or TCP, the HTTP 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 router 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 **telsh** 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.

- 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.

- 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
```

- CSCei49850

Symptoms: The **ip dhcp client update** command is not accepted on subinterfaces.

Conditions: This symptom is observed on a Cisco router when you attempt to configure Dynamic DNS.

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: There is no workaround.

- CSCei73629

Symptoms: A router may fail to obtain a valid router certificate if on startup the router's certificate is expired and the router has a shadow CA certificate.

Conditions: This symptom has been observed when the router's certificate is expired and the router has a shadow CA certificate.

Workaround: Delete the trustpoint and re-created it. Note that this action also deletes the CA and router certificates so the newly created trustpoint will have to be authenticated and enrolled.

- 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>.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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_SUPPRESS
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 behaviour 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".

- 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.

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.

- 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.

- 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.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(2)T2

Cisco IOS Release 12.4(2)T2 is a rebuild release for Cisco IOS Release 12.4(2)T. The caveats in this section are resolved in Cisco IOS Release 12.4(2)T2 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

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.

- 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.

- 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

- 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>.

- 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.

- 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.

- 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.

- 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: 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.

- 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. 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
```

- 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.

- 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 miscalculates 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.

- 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.

- 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.

- CSCei71944

Symptoms: The duration of the injected tone configured in the **voice-class tone-signal** command is shorter than the configured time. The shortest tone is on usually the last tone played.

Conditions: This symptom has been observed when the **voice-class tone-signal** command is configured on the Land Mobile Radio (LMR) port.

Workaround: Configure the command for 10 ms longer than what is actually needed for the last signal.

- CSCei73829

Symptoms: Cisco VPN Client 4.6.x connected to a Cisco IOS router configured as the VPN Server passes traffic correctly but after phase 2 SA rekeys, repeated phase 2 SA rekeying occurs and the Cisco VPN Client disconnects. The client log shows:

```
2007 20:18:34.732 08/06/05 Sev=Warning/2 IKE/0xE3000099
Immature Navigation Termination due to error (Navigator:195)
```

The router debug shows:

```
IPSEC(update_key_lifetimes): volume lifetime reached 0, dropping SA sibling
```

Conditions: This symptom has been observed with Cisco VPN Client 4.6.x connected to a router configured as the VPN Server and running Cisco IOS Release 12.4(2)T.

Workaround: Downgrade the router to Cisco IOS Release 12.4(3).

- 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.

- CSCei76753

Symptoms: BRI backhauling does not work on Cisco 2801 routers.

Conditions: This symptom has been seen on Cisco 2801 routers with Cisco IOS interim Release 12.4(02.02)T and Cisco IOS Release 12.4(2)T1. Backhauling works perfectly with Cisco IOS interim Release 12.4(1.9).

Workaround: There is no workaround.

- CSCin96534

Symptoms: Cisco 1800 series and Cisco 1810 series routers crash upon enabling dot1x.

Conditions: The crash has been seen only when enabling dot1x on an onboard FE interface and not on the switch ports.

Workaround: There is no workaround.

- CSCsa60223

Symptoms: After a call is made between H.323 and SIP on the IPIPGW, executing the **show call active voice** command does not reflect the call leg information.

Conditions: This symptom occurs when doing SIP-H323 calls.

Workaround: There is no workaround.

- CSCsa61115

Symptoms: After upgrading from Cisco IOS Release 12.3 mainline to Cisco IOS Release 12.3T, some information is not getting passed along correctly that is causing failures, for example third party Message Waiting Indication (MWI).

Conditions: This problem is seen when routers are upgraded to Cisco IOS 12.3T when QSIG signaling is used.

Workaround: Downgrade all routers involved to a version prior to Cisco IOS 12.3 (4)T.

- 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 expect 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.

- 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.

- CSCsa74930

Symptoms: A Cisco 3825 or Cisco 3845 router 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) and is mostly seen with Appletalk protocol over GE.

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.

- 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:

```
HDL32_RX_ISR_ERR: no particles available!
```

```
HDL32_RX_ISR_ERR: no particles available!
```

```
HDL32_RX_ISR_ERR: no particles available!
```

```
HDL32_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.

- 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.

- 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 addressx.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.

- 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.

- 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.

- 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.

- CSCsb33535

Symptoms: NAT translation fails in VPN Client mode over a period with traffic. NAT always takes the previously assigned IP address for the translation and traffic stops following through the EzVPN tunnel.

Conditions: This symptom has been observed in VPN Client mode.

Workaround: Reload the router. Otherwise, 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.

- 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 be removed for the host/cef-exception/transit path control-plane policing policy to work.

- CSCsb42436

Symptoms: In a remote access IPSec scenario using EzVPN clients to connect to a Cisco IOS router, the router crashes with an address error as soon as the ISAKMP idle timer expires. It appears that the timer expires and terminates the session, which causes the error and subsequent crash.

Conditions: This symptom has been observed when the ISAKMP idle time is configured. If the ISAKMP idle time is not configured, the crash does not occur.

Workaround: Do not configure idle time for ISAKMP.

- 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.

- 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 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.

- CSCsb56224

Symptoms: A buffering problem occurs on the AUX line on the Cisco 851 and Cisco 871 routers. The last character of AT commands from router AUX line (line 1) is displayed only after the first "RETURN" character. After the second "RETURN" character, the AT command is executed by the analog modem. This behavior is causing problems with chat scripts and sending AT commands to analog modem, making dial out impossible using chat scripts. It is possible to send AT commands to the modem using reverse telnet (AUX port). After each command, the "enter" key must be pressed twice. Even entering command characters like AT, the letter A is echoed after pressing T, T is echoed after next character, and so on.

Conditions: This symptom affects the AUX functionality of the Cisco 851 and Cisco 871 routers. Dial backup and remote management are not possible in these routers.

Workaround: There is no workaround.

- CSCsb59813

Symptoms: The H323-SIP gateway rejects valid SUBSCRIBEs with a '481 Call Leg/Transaction Does Not Exist' response message. The gateway may also crash.

Conditions: This symptom has been observed after the gateway receives an INVITE with Replaces header for a call that has an active subscription, and then subsequent SUBSCRIBE requests are received for that call.

Workaround: There is no workaround.

- CSCsb69726

Symptoms: 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 back server feature and is applicable only for Cisco VPN 3000 Concentrator with 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\nl". 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.

- CSCsb84615

Symptoms: The error message appears on a Cisco 1812 router during high traffic load.

```
*Sep  9 04:54:38.468: %MOTCR-3-CMD_ERR: MOTCR command returned error: (0x1048)
*Sep  9 04:54:38.468: motcr_lopri_error: unknown error 0x1048
*Sep  9 04:54:38.468: IPSECcard: an error coming back 0x1048
*Sep  9 04:54:38.688: %MOTCR-3-CMD_ERR: MOTCR command returned error: (0x1048)
*Sep  9 04:54:38.688: motcr_lopri_error: unknown error 0x1048
*Sep  9 04:54:38.688: IPSECcard: an error coming back 0x1048
*Sep  9 04:54:38.912: %MOTCR-3-CMD_ERR: MOTCR command returned error: (0x1048)
*Sep  9 04:54:38.912: motcr_lopri_error: unknown error 0x1048
*Sep  9 04:54:38.912: IPSECcard: an error coming back 0x1048
```

Conditions: This symptom has been observed on Cisco 180x and Cisco 181x routers with Cisco IOS Release 12.4(2)T, Release 12.4(2)T1, Release 12.4(2)YI, Release 12.4(2)YT, and Release 12.4(2)XA and with the k9 images.

Workaround: There is no workaround.

- CSCsb85920

Symptoms: The default route is added on the EzVPN server.

Conditions: When the inside interface has no IP address assigned or the cascaded ACL has the **ip any any** command, a default route gets pushed to the server which the server adds without validating.

Workaround: Ensure the inside interface has an IP address. Do not add the **ip any any** command to a cascaded network access-list.

- CSCsb85927

Symptoms: Previous routes on the EzVPN server are not deleted when the EzVPN client reconnects.

Conditions: This symptom has been observed when the old routes are not deleted when a new connection from the same peer is received. This situation happens when the session is not closed properly by the client.

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.

Wide-Area Networking

- CSCeg82698

Symptoms: PPTP tunnels do not come up.

Conditions: This symptom is observed when VPDN 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.

- CSCei21549

Symptoms: A Cisco AS5850 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.

Resolved Caveats—Cisco IOS Release 12.4(2)T1

Cisco IOS Release 12.4(2)T1 is a rebuild release for Cisco IOS Release 12.4(2)T. The caveats in this section are resolved in Cisco IOS Release 12.4(2)T1 but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- 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.

- 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>.

- 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.

- 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 dlc* 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.

IP Routing Protocols

- 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 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 is platform-independent and may also occur in other releases.

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.

- 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.

- 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.

- 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.

Miscellaneous

- 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/EPPII, 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/EPPII-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.

- 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. The symptom may also occur in other releases.

Workaround: Move the complete QoS configuration to the QoS policy on the main interface (that is, use an hierarchical policy).

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCei42520

Symptoms: When an E&M voice interface card (VIC) is installed in the High-Speed WAN Interface Card (HWIC) slot of an Integrated Services Router (ISR), the **bootup e-lead off** voice-port configuration command does not function.

Conditions: This symptom is observed on a Cisco 2800 series and Cisco 3800 series.

Workaround: There is no workaround.

- CSCei44616

Symptoms: When a Cisco EtherSwitch 4-port or 9-port high-speed WAN interface card (HWIC-4ESW or HWIC-D-9-ESW) is used with an PWR-2801-AC-IP power supply, no power is supplied to Power-over-Ethernet (PoE) devices.

Conditions: This symptom is observed on a Cisco 2811.

Workaround: Use an external power supply.

- CSCin94359

Symptoms: An EzVPN client does not propose AES as encryption algorithm during ISAKMP negotiation, though it is supported on a router that runs Cisco IOS software.

Conditions: This symptom is observed when AES is configured on the EzVPN server side.

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 than a 32-bit mask.

Workaround: Avoid using the RADIUS Framed IP Netmask Attribute or use a 32-bit mask value for it.

- 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.

- 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.

- 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/xxxxxxxxxxxxx/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) but may also occur in Release 12.3 or Release 12.4T.

Workaround: There is no workaround.

- 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.

- 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.

- CSCsb43655

Symptoms: Some incoming packets that are larger than 1400 bytes are incorrectly counted as “input errors” on an ATM interface. An ATM error debug reports an “ATM0: AAL5 rx errors (status = 0C100000)” message, which suggests congestion occurs while cells pass through the ATM interface.

Conditions: This symptom is observed on a Cisco 870 that is configured as an PPPoE client or for RFC1483 bridging. Note that the symptom does not occur on a Cisco 836.

Workaround: There is no workaround.

Further Problem Description: When the connected DSLAM is configured to mark some or all packets that are larger than 1400 bytes with the CNG bit (indicating a possible congestion), the Cisco 870 should not mark these packets as errors and should not drop these packets but should increase the congestion counters and process the packets normally if sufficient bandwidth is available.

Wide-Area Networking

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(2)T

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

Basic System Services

- 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).

- 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.

- CSCeh53673

Symptoms: The router pauses indefinitely during processing the default configurations of **l3 cache disable**.

Conditions: This symptom has been observed when the router loads the image and processes the default configuration.

Workaround: Load an working image and configure **no cache l3 disable**. This command will not disable l3 cache. For the command to be effective, reload the router. Boot the effected image as usual and this problem will not be seen.

- CSCeh64791

Symptoms: Memory may leak 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.

- 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.

- 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.

Interfaces and Bridging

- 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.

IP Routing Protocols

- 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.

ISO CLNS

- CSCsa90719

Symptoms: A router running Cisco IOS software will reload unexpectedly, when the **no passive-interface** command is issued under the **router isis** configuration.

Conditions: This symptom has been observed when the interface is configured to run ISIS and later changed to passive interface.

Workaround: Disable ISIS on the interface before changing it to passive, using the **no ip router isis** interface 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.

- 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
```

- 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.

- 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.

- 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.

- 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.

Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13) or Release 12.3(11)T3. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCeh62596

Symptoms: Performing Telnet results in the session pausing indefinitely after accepting 13 characters or carriage returns.

Conditions: This symptom has been observed when performing a Telnet session through ATM PVC which is PPPoA but that a Telnet session through Fast Ethernet works fine.

Workaround: Avoid using Telnet session through ATM PVC which is PPPoA. Use Fast Ethernet for Telnet sessions if possible.

- 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 the 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.

- 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.

- 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.

- CSCeh80851

Symptoms: The **IPv6** commands and options under the **interface dot11radio slot/port/radio** command are seen and are configurable.

Conditions: This symptom has been seen in Cisco IOS Release 12.3(8)YI1. The command is not available in subsequent releases as it is not supported.

Workaround: The **IPv6** commands and options are not supported for any release after Cisco IOS Release 12.3(8)YI1. The unsupported commands and options should not be configured.

- 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.

- 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 Cisco AS5400 or Cisco AS5850.

- 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.

- 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.

- 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.

- 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 Cisco 2800 series that is configured for encryption, CBAC, and IPS crashes and reloads during the inspect process.

Conditions: This symptom is observed on a Cisco 2800 series that runs Cisco IOS 12.3T when it functions under a heavy load of mixed application traffic and IP telephony traffic.

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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsa90842

Symptoms: Transparent IPS and Transparent Firewall functionality is missing from certain Cisco IOS images for the Cisco 3725 and Cisco 3745 routers.

Conditions: This functionality can not be used on the following images:

- c3725-adventerprise9-mz
- c3725-adventerprise9_ivs-mz
- c3725-adventerprise9_sna-mz
- c3745-adventerprise9-mz
- c3745-adventerprise9_ivs-mz
- c3745-adventerprise9_sna-mz

Workaround: To use this functionality, use the following images:

- c3725-advsecurityk9-mz
- c3725-advipservicesk9-mz
- c3745-advsecurityk9-mz
- c3745-advipservicesk9-mz

- 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.

- 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.

- CSCsa99597

Symptoms: Reload is caused by memory corruption.

Conditions: This symptom has been observed when the router is a Cisco IPSec gateway which implements XAUTH. One example of this situation is a Cisco EZVPN server.

Workaround: There is no workaround.

Further Problem Description: The problem occurs if the username given to XAUTH is exactly 7, 19 or 43 characters long (given a default configuration). The exact lengths which tickle the symptom may vary depending on the **memory lite** configuration.

- 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.

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.

- 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.

- 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.

- 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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with [Release Notes for Cisco IOS Release 12.4 T](#).

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.

