Caveats for Cisco IOS Release 15.1(1)T

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

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

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

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

Resolved Caveats—Cisco IOS Release 15.1(1)T5

Cisco IOS Release 15.1(1)T5 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T5 but may be open in previous Cisco IOS releases.

- CSCsx87562

  ```
  Symptoms: The following error is seen following interface range configuration change:
  %SYS-3-TIMERNEG: Cannot start timer (0xXXXXXXXX) with negative offset (- YYYYYYYYYY).
  -Process= "<interrupt level>", ipl= 2
  ```

  Conditions: This symptom is seen with dual supervisors installed and affects the following Cisco Catalyst 4000 releases: Cisco IOS Release 12.2(52)SG/XO, Cisco IOS Release 12.2(50)SG4/5/6/7, and Cisco IOS Release 12.2(53)SG/SG1/SG2. This bug applies to all hardware, and is not specific to Cisco Catalyst 4500 series switches.

  Workaround 1: Configure the interfaces one by one.

  Workaround 2: Force a switchover "redundancy force-switchover".

  Workaround 3: Use Cisco IOS Release 12.2(50)SG3 until the fix code is released.

  Resolution: The fix is available in Cisco IOS Release 12.2(54)SG which is available to download on CCO. The fix will also be in Cisco IOS Release 12.2(53)SG3 and Cisco IOS Release 12.2(50)SG8.

- CSCte53162

  Symptoms: In radius messaging, nas-port-id is not prepended to "acct-session-id" when the **nas-port format e** *encoding string* command is configured.

  Conditions: This symptom is observed when the **nas-port format e** *encoding string* command is configured.

  Workaround: Use the **nas-port format d** *encoding bits* command.

- CSCte97113

  Symptoms: The **configure replace** command fails and crashes the standby when you try to replace an existing configuration on the active that has parser views configured with a configuration that does not have any parser views configured.

  Conditions: This symptom is observed when the user is in root view mode while configuring a parser view. During configure replace, the standby is not set into root view mode.

  Workaround: Manually remove/configure the parser view on the active to match with what it is in the saved configuration before opting for configure replace.

- CSCtf49537

  Symptoms: During the bulk-sync, Standby does not reload when a configuration command with parser return code error is seen on Standby. The user will not notice if a PRC error occurred.

  Conditions: This symptom is observed when the PRC error result status is not sent back from Standby to Active properly.

  Workaround: After the system reaches the SSO state, issue the following exec command via the Active console to check if PRC error occurred.

  ```
  router# show redundancy config-sync failures prc
  ```

- CSCtf71990

  Symptoms: An alert message is not sent if "source-ip-address" is configured in the call-home configuration. The following message is shown:

  ```
  %CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP
  ```

```
servers (ERR 7, error in connecting to SMTP server)
```

Conditions: The symptom is observed when “source-ip-address” is configured.

Workaround: Remove “source-ip-address”.

- CSCtg79262

  Symptoms: A Cisco IOS Embedded Event Manager (EEM) Tool Command Language (Tcl) policy can get stuck in the EEM active scheduler queue. The policy will consume a scheduler thread and cannot be cleared automatically by the maxrun timer or manually using the EEM exec command **event manager scheduler clear all**.

  Conditions: This symptom occurs in very rare circumstances. For example, if the system has enough memory to schedule and start running the EEM policy, but the policy fails due to a lack of memory.

  Workaround: The only way to recover is to reload.

- CSCtg91572

  Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

  Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

  Workaround: There is no workaround.

- CSCth43911

  Symptoms: The system may crash when performing the SNMP SET operation for CISCO-CALLHOME-MIB objects in callHomeDestEmailAddressTable, ccmSeverityAlertGrouptable, ccmPeriodicAlertGroupTable, ccmPatternAlertGroupTable, ccmEventAlertGroupTable, and ccmDestProfileTestTable.

  Conditions: This symptom does not occur under any specific conditions.

  Workaround: There is no workaround. The fix exists in Cisco IOS Release 12.2(33)SXJ and Cisco IOS Release 12.2(50)SY.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate the video stream.

  Conditions: This symptom is observed in two scenarios:

  Scenario 1: This symptom was observed in the following SIP-SIP Delayed Offer-Delayed Offer (DO-DO) call flow :

  ```
  7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server
  ```

  1. Call is originated by 7985.
  2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response.

```
m=video 53722 RTP/AVP 96 97 34 31
b=AS:1920
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600
a=rtpmap:97 H263-1998/90000
a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1
a=rtpmap:34 H263/90000
a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1
a=rtpmap:31 H261/90000
a=fmtp:31 CIF=1;QCIF=1
```

```
a=sendrecv
```

3. CUBE sets video m-line to 0 in the SDP of the SIP “ACK” response

```
m=video 0 RTP/AVP 96
```

Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

```
CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA
```

Workaround: There is no workaround.

- CSCth84370

  Symptoms: The Standby Supervisor gets reloaded when **write memory** is run from one VTY, and then later, **show configuration** is run from another VTY. No particular configuration needs to be done prior to **write memory**.

  Conditions: This symptom occurs when the Dual Supervisor is used and the configuration file is quite long.

  Workaround: Do not run the **write memory** and **show configuration** commands simultaneously.

- CSCth92828

  Symptoms: When viewing a device configuration, such as via a URL like https://tools.cisco.com/sch/reports/viewDeviceConfiguration.do<specific_item_quer y>, the TACACS server key, a type 7 reversible password, is still visible.

  Conditions: This symptom is observed when viewing a device configuration.

  Workaround: There is no workaround.

- CSCti08811

  Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- CSCti41891

  Symptoms: When 812 tunnels are configured, Standby starts rebooting.

  Conditions: This symptom is observed with scalability.

  Workaround: There is no workaround.

- CSCti46171

  Summary: The Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  – Memory Leak Associated with Crafted IP Packets.

  – Memory Leak in HTTP Inspection.

  – Memory Leak in H.323 Inspection.

  – Memory Leak in SIP Inspection.

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The

Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-1315 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtj48387

  Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP-related errors.

  Conditions: This symptom occurs when DHCP is enabled and sessions get DHCP information from a RADIUS server.

  Workaround: There is no workaround.

- CSCtn55070

  Symptoms: Call-home http messages can hang and not be sent out.

  Conditions: This symptom is observed when call home is enabled and an http transport method is used. This symptom is timing-dependent and cannot be hit every time. In addition, this symptom is observed in telnet sessions.

  Workaround: Log in to the console port if a telnet session was used to send call-home http messages. Because the console is waiting on user- supplied information (--More--), enter something into the console; the call-home process can then continue to execute.

- CSCtq06538

  Symptoms: A Cisco ASR with a route processor 2, running Cisco IOS XE, may experience RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing Codenomicon BGP tests.

  Workaround: There is no workaround.

  Additional Information: This crash was only seen in some 15.x versions of Cisco IOS XE. It is due to a malformed BGP attribute received from a valid BGP neighbor. This attribute is not passed on to any systems other than the vulnerable router.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.7/4.5:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C

  CVE ID CVE-2012-1367 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq45553

  Summary: The Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets.
  - Memory Leak in HTTP Inspection.
  - Memory Leak in H.323 Inspection.
  - Memory Leak in SIP Inspection.

  Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-0388 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq92650

  Symptoms: DMVPN tunnel is not selecting the right source interface.

  Conditions: The symptom is observed when multi-link frame relay creates more than one sub-interface with the same name.

  Workaround: There is no workaround.

  Further Problem Description: This bug resolves the issue reported in CSCth08338 for Cisco IOS Release 15.1M.

- CSCtr28857

  Summary: A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of the Cisco IOS Software and the Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication'' at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr54327

  Symptoms: A Cisco router may crash due to a SegV exception or may have spurious access when a fax comes in.

  Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the "a=silenceSupp:off" option is set in SDP.

Workaround: Disable fax by going into the “voice service voip” mode and configuring the **fax protocol none** command.

- CSCts38429

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

- CSCts80643

  The Cisco IOS Software and the Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, and not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt94391

  Symptoms: A Cisco wireless router may unexpectedly reboot due to a bus error with the following error leading up to the crash:

  ```
  ASSERTION FAILED: file ''../dot11t/t_if_dot11_hal_ath.c'', line XXXX
  ```

  Conditions: This issue relates to the wireless on the router. This crash can be seen on the following platforms: Cisco 870W, 1800W, UC500W, and 2800 and 3800 routers with HWIC-AP. The crash is only seen when an iPhone 4S is connected to the router. The crash has most commonly been triggered by running a video call application on the phone, but there may be other triggers. Other than the wireless configuration and other generic configurations needed to provide connectivity to the router, no other specific configuration is needed to see the crash.

Workaround: There is no workaround on the router. However, this issue is not seen with an iPhone 4s running iOS 5.1. The issue is only seen on iOS 5.0.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C

CVE ID CVE-2012-1327 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtu02835

  Symptoms: While running Cisco IOS Release 15.1(4)M2, slow performance is exhibited through the Fast Ethernet WAN ports.

  Conditions: This symptom is observed when the **scheduler interval** command is configured. This causes the Fast Ethernet WAN ports to display many throttles in the **show interface** command.

  Workaround: Remove the **scheduler interval** command.

- CSCtu36224

  Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

  Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.

  Workaround: There is no workaround.

- CSCtx38806

  Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

  This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

  The problem affects Firefox also (version 10.0.1) displaying the following message:

  "The page isn't redirecting properly."

  Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.

  Workaround: Any of the following workarounds will work:

  1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
  2. Uninstall the update.
  3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

```
webvpn gateway gateway name
  ssl encryption rc4-md5
```

  4. Use AC 2.5.3046 or 3.0.3054.
  5. Use older versions of Firefox (9.0.1).

  Further Problem Description: For AnyConnect users, the following user error message is seen:

  "Connection attempt has failed due to server communication errors. Please retry the connection."

  The AnyConnect event log will show the following error message snippet:

```
Function: ConnectIfc::connect
Invoked Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCty42626

  Symptoms: Certificate enrollment fails for the Cisco 3945 router and the Cisco 3945E router due to digital signature failure.

  Conditions: This symptom is observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  Workaround: There is no workaround.

- CSCty43587

  Symptoms: A crash is observed with memory corruption similar to the following:

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

  Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(1)T4

Cisco IOS Release 15.1(1)T4 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T4 but may be open in previous Cisco IOS releases.

- CSCso46409

  Symptoms: "mbrd_netio_isr" and "crypto_engine_hsp_hipri traceback" log messages are produced.

  Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM- VPN/SSL-3.

  Workaround: There is no workaround.

- CSCta11223

  Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

  Conditions: This symptom is observed when the device is running Cisco IOS software and is configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

  Workaround: There is no known workaround.

- CSCtb32043

  Symptoms: CPUHOG messages may be displayed or the Cisco IOS software might crash when executing no ipv6 multicast-routing in a configuration with more than 20,000 IPv6 multicast-enabled interfaces or subinterfaces.

Conditions: This symptom is observed only rarely when an alternate software path is taken. It is not known what causes this alternate path to be taken.

Workaround: There is no workaround.

- CSCtb55479

  Symptoms: A router may crash by the “BGP Router” process.

  Conditions: This symptom is observed if the memory is corrupted.

  Workaround: There is no workaround.

- CSCtb72734

  Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

  Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

  Workaround: There is no workaround.

- CSCtb74547

  Symptoms: A Cisco ASR 1000 DMVPN HUB reloads at the process IPSEC key engine.

  Conditions: This symptom is observed when the “Dual DMVPN with Shared Tunnel- Protection” feature is enabled and the interface is shut down and brought up again.

  Workaround: There is no workaround.

- CSCtc49086

  Symptoms: When configuration changes are performed within a multicast-enabled VRF that cause the PIM register tunnel interface to go down and up again, spurious memory access appears when traffic is sent at the same time.

  Conditions: This symptom occurs when traffic is sent when configuration changes are performed.

  Workaround: There is no workaround.

- CSCtd23069

  Symptoms: A crash occurs because of a SegV exception after configuring the ip virtual-reassembly command.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCte27828

  Symptoms: Call forward does not work.

  Conditions: Topology: call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider.

  IP addresses: CUCM10.10.10.3 Cube SUD10.10.10.2 CUBE North192.168.101.10 SBC 192.168.100.5

  “Call forward no answer” scenario does not work, but not systematically: sometimes it works, sometimes not.

  When the “call forward no answer” fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC doesn’t answer due to this.

  Workaround: There is no workaround.

- CSCtf24052

  Symptoms: On a Cisco router loaded with Cisco IOS Release 15.0(1)M or Release 15.1(1)T, traffic may not match the ACL configured with a port range inside a class map.

  Conditions: This symptom is observed when port range ACE is configured after a few ACEs, as in the following example:

```
Flashcard# show access-lists 101

Extended IP access list 101
    10 permit icmp any any
    20 permit udp any any eq domain
    30 permit udp any eq domain any
    40 permit tcp any any range <start> <end>
    50 permit tcp any range <start> <end> any
<removed>
    220 permit tcp any any range <start> <end>
```

  Workaround: Use ACE with a specific port to match the traffic, or use IP source/destination.

- CSCtf32100

  Symptoms: Packets are dropped.

  Conditions: This symptom is observed with router-destined traffic on an interface with VRF and crypto map configured, when the hardware is Cisco 7200 G2 with VSA.

  Workaround: There is no workaround.

- CSCtf71673

  Symptoms: A Cisco 10000 series router shows a PRE crash due to memory- corruption with block overrun.

  Conditions: This symptom is seen when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

  Workaround: There is no workaround.

- CSCtf81249

  Symptoms: Memory leaks occur while configuring Cisco IOS commands.

  Conditions: This symptom is observed only when configuring from tclsh.

  Workaround: Use the **end** command specifically to avoid any leaks.

- CSCtg41206

  Symptoms: In a Cisco 7200VXR NPE-2 with VSA crypto accelerator enabled and GDOI crypto-map applied to an interface, egress QoS classification is not happening for non-encrypted packets. As the result, these packets end up in class-default and being treated accordingly. Packets/bytes/rate counters in class-default are not counting these packets properly. Encrypted packets are processed correctly.

  Conditions: This behavior is observed in all Cisco IOS Releases 12.4(24)T and 15.0(1)M.

  Workaround: Disable VSA crypto accelerator with the **no crypto engine slot 0** global configuration command. Switching to software crypto engine may adversely affect router's crypto processing performance, CPU load, and control plane stability.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtg68047

  Symptoms: The router reloads.

  Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

  Workaround: Wait until the tunnels are shut down before issuing the show command.

- CSCtg68208

  Symptoms: A router may repeatedly reload when an L2TPv3 xconnect configuration is present and there is no interface configured with an IP address.

  Conditions: This symptom has been observed when the **xconnect** command specifies **encapsulation l2tpv3**, and all interfaces on the router are either configured with **no ip address** or **ip address dhcp**.

  Workaround: To avoid this problem, ensure there is an interface that is able to reach the L2TPv3 peer and that has an IP address configured.

- CSCtg72652

  Symptoms: On Cisco 2900 series routers, the following warning message might display on the console:

  ```
  %ENVMON-1-POWER_WARNING: : Chassis power is not good in the PSU 1
  ```

  Conditions: Under rare conditions, the power supply sometimes sends a false alarm status to the system, even though the system power is working fine.

  Workaround: There is no workaround.

- CSCtg73604

  Symptom: E1R2 compelled signaling calls fail.

  Conditions: This symptom is observed when a call is made using E1R2 compelled signaling.

  Workaround: There is no workaround.

- CSCtg84969

  Symptoms: The output of **show ip mfib vrf <vrf name> verbose** may show the following line "Platform Flags: NP RETRY RECOVERY HW_ERR" and multicast traffic may not be hardware switched.

  Conditions: The symptom is observed on a dual RP Cisco 7600 series router with linecards after multiple reloads or SSO switchovers. When the issue occurs the output of **show ip mfib vrf <vrf name> verbose** on the standby SP will show some lines preceded with "###" where an interface name is expected.

  Workaround: There is no workaround.

- CSCtg89555

  Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

  Conditions: This symptom is observed when configuring an ip address after multicast has been configured on a dot1Q interface.

  Workaround: Performing a **shut/no shut** of the interface will fix the problem.

- CSCth01526

  Symptoms: MDT interface deactivated and activated after an SSO.

  Conditions: After an SSO switchover, the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

  Workaround: There is no workaround.

- CSCth01939

  Symptoms: IPsec packets are dropped on the router and an error is displayed on the console.

  Conditions: This symptom is observed on a Cisco IAD2430 with VPN/GRE tunnel configuration and AES256 encryption.

  Workaround: There is no workaround.

- CSCth11006

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  NetMeeting Directory (Lightweight Directory Access Protocol, LDAP) Session Initiation Protocol (Multiple vulnerabilities) H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCth28702

  Symptoms: This bug has been filed to enhance the code to follow secure best practices and enhance resiliency of the product.

  Conditions: Not applicable.

  Workaround: Not applicable.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCth45432

  Symptoms: Traffic that is CEF-switched through the router does not exit Async interfaces.

  Conditions: This symptom is observed with CEF enabled and in Cisco IOS Release 12.4(20)T and above with MFI.

  Workaround: Disable CEF or downgrade to Cisco IOS Release 12.4(15)T before MFI.

- CSCth84233

  Symptoms: Router may crash due to Redzone memory block corruption (I/O) when "qos pre-classify" is configured under tunnel interfaces. The packet is overwriting the next block.

  Conditions: The trigger for this issue is configuring "qos pre-classify".

  Workaround: Remove "qos pre-classify".

- CSCth85294

  Symptoms: A PIM neighborship is not established with the remote PE and RP for the MVRFs.

  Conditions: This symptom is observed with traffic and after removal and restoration of MVRFs. Traffic does not flow properly since the PIM neighborship is not established with the remote PE and RP for those MVRFs.

  Workaround: There is no workaround; however, multiple removals of MDTs could help.

- CSCth87458

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

  Conditions: This was experienced during internal protocol robustness testing.

  Workaround: Allow SSH connections only from trusted hosts.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2011-2568

  has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti01971

  Symptoms: The active router crashes during a switchover in a scaled BFD IPv6 setup.

  Conditions: The router is configured with a larger number of IPv6 routes with BFD sessions configured. (The test was done with 500 BFD IPv6 sessions.)

  Workaround: There is no workaround.

- CSCti18615

  Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP being out of sync with the active RP. The A and F flags are missing from the multicast forwarding base entries.

  Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, and when the router is in HA mode SSO and is reloaded from the RP.

Workaround: Perform a shut/no shut of the affected interfaces.

- CSCti35326

  The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.

  The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.

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

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-nat

- CSCti48483

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  NetMeeting Directory (Lightweight Directory Access Protocol, LDAP) Session Initiation Protocol (Multiple vulnerabilities) H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCti64685

  Symptoms: User may not be able to configure SLA MPLS configuration.

  Conditions: This symptom occurs when the router is booted up and may be random.

  Workaround: There is no workaround.

- CSCti81539

  Symptoms: Some of the ACLs related to TCP cannot be removed from a router.

  Conditions: This symptom is observed while unconfiguring ACLs.

  Workaround: Remove the entire ACL, and recreate it again.

- CSCti89976

  Symptoms: Standalone AnyConnect 3.0 client does not work with an existing IOS headend.

Conditions: The symptom is observed when AnyConnect 3.0 is used with an existing IOS headend.

Workaround: Use client versions less than or equivalent to 2.5, or use weblaunch.

- CSCti99419

  Symptoms: An HWIC-1DSU-T1 card is not recognized after a reload.

  Conditions: This symptom is observed on an HWIC-1DSU-T1 card after a reload. It occurs only about 1 to 2 percent of the time.

  Workaround: Power-cycle the router.

- CSCtj15798

  Symptoms: Some modems in PVDM2-xxDM module are marked as BAD after running clean for few days. The **show modem** command will report a "B" in front of the modem ("B - Modem is marked bad and cannot be used for taking calls").

  Conditions: The symptom is observed with the PVDM2-xxDM module.

  Workaround: Reloading the router gives another few days of clean connections before the issue comes back again.

- CSCtj23189

  Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.

  Conditions: This happens only when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with 3 classes: one with 16 kbps, second one with 1 Mbps, and the third one with 99 Mbps.

  Workaround: There is no workaround.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj39664

  Symptoms: A router that is running Cisco IOS Release 15.1(2)T1 may crash when attempting to configure Zone-Based Firewall.

  Conditions: The symptoms are observed when attempting to configure zone-pair. It occurs only with a Cisco 861 router.

Workaround: There is no workaround.

- CSCtj46670

  Symptoms:

  IPCP cannot complete after dialer interface is moved out of Standby mode CONFREJ is seen while negotiating IPCP

  Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

  Workaround: Reload the router.

- CSCtj47696

  Symptoms: A Cisco router supporting HWIC-2CE1T1-PRI WAN module will not process any in/outgoing ISDN calls once the network derived clock is configured (i.e.: "network-clock-participate wic 0").

  Conditions: The symptom is observed on a Cisco 3800/3900 series router with NM-8CE1T1-PRI, HWIC-2CE1T1-PRI or VWIC3-2MFT-T1/E1 running Cisco IOS Release 15.1 (1)T or Release 12.4(24)T4 deriving the clock from the network.

  Workaround: Configure "national reserve 0 0 0 0 0 0" under the affected E1 port following by shut/no shut of the E1 port. Complete the workaround by configuring "national reserve 1 1 1 1 1 1" and flapping the port one more time.

  If modem calls are not required, "no network-clock-participate" can also be used as a workaround.

  Further Problem Description: Problem is not seen on VWIC2-2MFT-T1/E1.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj79676

  Symptoms: The router crashes sometimes once CEF is enabled.

  Conditions: This symptom occurs when CEF is enabled.

  Workaround: There is no workaround.

- CSCtj84234

  Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

  Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBRed in hardware. This symptom is observed with route-map configuration, as given below:

  route-map <RM name>
  match ip address <acl>
  set ip next-hop <NH1> <NH2>

  Workaround: There is no workaround.

- CSCtj95685

  Symptoms: A router configured as a Voice Gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a Voice Gateway.

Workaround: There is no workaround.

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

  Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

  Workaround: There is no workaround.

- CSCtk01638

  Symptoms: Analog endpoint and connection trunk is torn down due to the following Q.850 cause code in SIP BYE request:

  Port will show in a S_TRUNK_PEND
  ****
  show voice call summary | include 0/2/0
  0/2/0- - - S_TRUNK_PEND

  Conditions: This symptom is observed when the **clear counters** command is invoked. This triggers the gateway to stop sending rtcp events, which causes media inactivity to be activated on the far-end gateway and the connected trunk to be torn down.

  Workaround: There is no workaround.

- CSCtk02814

  Symptoms: The **show pppoe throttled subinterfaces** command output is truncated, and does not show throttled ATM VC or QinQ subinterfaces during throttling.

  Conditions: This symptom occurs when pppoe throttling is configured and active.

  Workaround: There is no workaround.

- CSCtk13720

  Symptoms: A Cisco router may crash when trying to remove an entry from an extended access-list.

  Example:

  ```
  Extended IP access list < NAME >
      10 permit tcp any any ack
      20 permit tcp any any fin
      30 permit tcp any any ack fin
      40 permit tcp any any rst
  Router (config)# ip access-list extended < NAME >
  Router (config-ext-nacl)# no 10
  ```

  Conditions: This symptom was first found on a Cisco router running Cisco IOS Release 15.0(1)M4 with extended access-lists and QoS configured. After further testing, we were able to determine that Cisco IOS Release 15.1(3)T did not crash due to this bug.

  Router will crash only if we have TCP flags in the ACL.

  Workaround: To modify an ACL, follow these steps:

  1) Remove ACL filter from the class. For example:

  ```
  class-map match-any c1
    no match access-group name QOS-TCP-OPTIONS
  ```

  2) Modify the ACL:

  ```
  ip access-list extended QOS-TCP-OPTIONS
    no 10
  ```

3) Re-add the ACL filter in class:

```
class-map match-any c1
  match access-group name QOS-TCP-OPTIONS
```

So basically, *do not* modify ACL if the ACL is configured as a filter under any class. Remove filter first, modify ACL and re-add filter to class.

- CSCtk32975

  Symptoms: The system crashes.

  Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

  Workaround: There is no workaround.

- CSCtk67709

  Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:

  ```
  ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432- k9.pkg
  SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
  ```

  Conditions: This symptom is observed with AnyConnect 3.0.

  Workaround: There is no workaround.

- CSCtk67934

  Symptoms: A Cisco router is forced to reload after a few days of encryption and decryption while processing high traffic.

  Conditions: This symptom is observed when VSA is enabled as a hardware crypto engine used for processing both firewall and encryption/decryption on the same interface.

  Workaround: Switch from VSA HW crypto engine to either SW crypto engine or VAM2+ HW crypto engine.

- CSCtk74685

  Symptoms: When H225 messages for a call are sent out to the wrong TCP socket by a Cisco IOS gateway, they may sent to a completely different IP than the one that is aware of the call. When this occurs, the new socket gets paired to the call and the H323 stack tries to tear down the H245 socket for a call that is being disconnected. Instead, it erroneously tears down an unrelated calls H225 socket. This causes the unrelated call to drop.

  Observed with “debug cch323 all” and “debug ip tcp trans:”

  ```
  13090333: Dec 3 13:18:20.965: //137091/80C6B1F78F31/H323/run_h245_iwf_sm: received
  IWF_EV_H245_DISCONN while at state IWF_ACTIVE 13090334: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_send_event_to_h245_connection_ sm: Changing to new
  event H245_DISCONNECT_EVENT 13090335: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_h245_connection_sm: state=0, event=4,
  ccb=C5E442B8, listen state=2 13090336: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_h245_connection_sm: H245_CONNECT: Received event
  H245_DISCONNECT_EVENT while at H245_NONE state 13090337: Dec 3 13:18:20.965: TCP0:
  state was ESTAB -> FINWAIT1 [24696 -> 192.0.2.100(1720)] 13090338: Dec 3 13:18:20.965:
  TCP0: sending FIN
  ```

  Conditions: This symptom occurs with all IOS images with the fix for CSCin76666.

  The cascade issue noted in this bug is triggered by an event where CM closes down an H225 or H245 TCP socket mid-call. Due to the cascading nature of CSCtk74685, identifying the root call that triggers this socket conflict may be extremely difficult, until the fix for CSCtk74685 is applied.

  Workaround: Use one of the following workarounds:

1. Enable call preservation on CM, which does not prevent the socket from getting torn down, but minimizes user impact and does not drop audio on the call.

voice service voip h323 call preserve

System > Service Parameters > (Select Publisher Node) > Cisco CallManager > Advanced > Allow Peer to Preserve H.323 Calls > False > Save

2. Run a Cisco IOS release that does not have the fix for CSCin76666.

3. Change the signaling protocol to SIP.

- CSCtl20509

  Symptoms: CME/SRST 4.0 when ATA unregister/ fall back to Cisco Unified CallManager, the virtual POTS dial-peers stay up and calls to ATA do not go out the H323 dial-peer to Cisco Unified CallManager. The calls fail with user busy. This issue affects only ATA. Dial peers of the IP phones behave normally.

  Conditions: This symptom occurs when the ATA fallback to the CCM occurs and registers with the CCM. However, The virtual pots dial peer for the ATA are up.

  Workaround: Reload the router.

- CSCtl45684

  Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

  ```
  ASSERTION FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 726 ASSERTION
  FAILED: file "../hwic/shdsl_efm/if_hwic_shdsl_efm_io.c", line 30
  ```

  Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.

  Workaround: There is no workaround.

- CSCtl54975

  Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

  Conditions: Unknown.

  Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl67079

  Symptoms: Following error message is seen on Cisco router with HWIC_1GE_SFP inserted:

  ```
  %HWIC_1GE_SFP-3-INTERNAL_ERROR: GigabitEthernet0/0/0 SNMP high capacity counter
  register failed
  ```

  Conditions: This symptom is observed during bootup.

  Workaround: There is no workaround.

- CSCtl87879

  Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

  Workaround: There is no workaround.

- CSCtl95752

  Symptoms: HWIC-4SHDSL-E reports erroneous EOC and PBO values over time.

  Conditions: This symptom is observed when the HWIC-4SHDSL-E port is connected to the Alcatel-Lucent DSLAM.

  Workaround: There is no workaround.

- CSCtn08208

  Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.

  Workaround: Downgrade to Cisco IOS Release 15.0(01)M2.4.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn12119

  Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

  Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

  Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn16855

  Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

  Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

  Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn19496

  Symptoms: Packet loss is seen when the service policy is applied on the tunnel interface. The **show hqf interface** command output shows drops in a particular queue with the following:

  Scheduler_flags 177

  The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.

  Conditions: This symptom is observed when the service policy is applied on the tunnel/GRE interface, and when the source of the tunnel interface is the ATM interface(hwic-shdsl).

  Workaround: There is no workaround.

  Further Problem Description: The above-described symptom is seen only with the SHDSL link.

- CSCtn48744

  Symptoms: Memory leaks on OER border router while running PfR-IPSLA configuration.

  Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtn68643

  Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

  Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption.

  ```
  ipv6 ospf encryption ipsec spi 500 esp null sha1
  123412341234123412341234123412341234123412341234
  ```

  or

  ```
  ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
  ```

  Workaround: There is no workaround.

- CSCtn72939

  Symptoms: The L2tpv3 feature is not working on Cisco c181x platforms.

  Conditions: This symptom occurs with Cisco c1812 running Cisco IOS Release 15.(0)M and later releases.

  Workaround: Configure bridge-group under that xconnect interface.

- CSCtn74673

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.

  Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.

  Workaround: There is no workaround other than line card reload.

- CSCto07919

  Symptoms: Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload.

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload.

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCto08135

  Symptoms: When a deny statement is added as the first ACL, the message gets dropped.

  Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.

  Workaround: Turn off the VSA, and go back to software encryption.

- CSCto08754

  Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.

  Conditions: This symptom occurs when the crypto VTI interface becomes wedged.

  Workaround: There is no workaround.

- CSCto13254

  Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error: Hash verification failed for file <temp location of profile>

  Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

  Workaround: Remove the profile from the Cisco IOS headend.

- CSCto14435

  Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

  Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

  Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto41173

  Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.

  Conditions: This symptom is observed with a platform that acts as an H323 gateway and runs Cisco IOS Release 15.1(3)T.

  Workaround: Revert to Cisco IOS Release 12.4(20)T.

- CSCto53332

  Symptoms: A router configured for IPSEC accounting may display the following error message:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  This does not seem to result in any impact apart from intermittently lost accounting messages.

  Conditions: This symptom occurs when ipsec accounting is active.

  Workaround: There is no workaround.

- CSCto55643

  Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

  Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

  Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

  Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

Workaround: There is no workaround.

- CSCto63268

  Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.

  Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

  Workaround: Remove the EVM or disable DSP sharing.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

  Conditions: This symptom is seen with GETVPN related configurations with fail-close feature activated.

  Workaround: There is no workaround.

- CSCto68554

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

  – Memory leak in Cisco IOS Software

  – Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw.

- CSCto72480

  Symptoms: The output of the **show mfib linecard** command shows that line cards are in “sync fail” state.

  Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

  Workaround: If this issue is seen, using the **clear mfib linecard** *slot* command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

  Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto72927

  Symptoms: Configuring an event manager policy may cause a cat4k to hang.

  Conditions: Configuring a TCL policy and copying that policy to the device.

Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.7/3.1:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C No CVE ID

has been assigned to this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCto86833

  Symptoms: The router's CPU spikes to 100 percent, leading to voice call failures, among other problems.

  Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DNs with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router's average CPU will be around 50 to 60 percent.

  Workaround: If possible, reduce the number of voice ports automatically generated by the number DNs and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the **show voice port summary** command to view the total number of voice ports created on the router after SRST configuration.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCto93837

  Symptoms: Cisco IOS may experience a memory leak when parsing certain responses to an outgoing SUBSCRIBE.

  Conditions: Cisco IOS is configured to process SIP messages.

  Workaround: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2011-4019 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq05004

  Symptoms: A dialer loses its IP address sporadically. The **show interface atm x** will record output drops during the issue. ATM0 is up, line protocol is up:

  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 31956 << Incrementing during the issue

  The **show interface queueing atm0.1** hidden command will show as follows:

  ```
  Interface ATM0 VC 8/35 Queueing strategy: fifo Output queue 40/40, 31956 drops per VC
  << Incrementing during the issue
  ```

  During the issue, if "debug ppp negotiation" is on, we will see the following:

  ```
  PPP: Missed 5 keepalives, taking LCP down PPP DISC: Missed too many keepalives
  ```

  There will be no ATM (physical interface) flap in this case (during the issue).

  A shut/no shut on the ATM interface does not help.

  Conditions: No conditions so far. The behavior is sporadic.

  Workaround: Reload.

- CSCtq05636

  Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg. For example:

  Received: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0

  Sent: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0

  In Cisco IOS Release 15.1.3T1, the * character is not forwarded.

  Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.

  Workaround: Upgrade the code to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

- CSCtq07413

  Symptoms: A hardware crypto engine may fail to decrypt packets. An "invalid parameter" error is seen after decryption. Software encryption works fine.

  Conditions: This symptom is observed in Cisco IOS Release 12.4.15T6.

  Workaround: Use software encryption.

- CSCtq09899

  Symptoms: The VXML gateway crashes.

  Conditions: This symptom occurs during the load test, when the **show mrcp client session active** is used.

  Workaround: There is no workaround.

- CSCtq10684

  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

  Conditions: This symptom occurs when tunnel flap is observed before the crash.

  Workaround: A possible workaround is to reload the box.

- CSCtq12007

  Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

  Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less sever; you may see one every other packet drop, until the next rekey or tunnel reset.

  Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

  Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq15247

  Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.

  Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.

  Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

  For example:

```
LAC1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
LAC1(config)# interface virtual-ppp1
LAC1(config-if)# no pseudowire
LAC1(config-if)# exit
LAC1(config)# no interface virtual-ppp1
```

- CSCtq24733

  Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.

  Conditions: The symptom is observed with MRCP is enabled.

  Workaround: There is no workaround.

- CSCtq27180

  Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.

  Conditions: This symptom is observed only on IOS internal releases.

  Workaround: There is no workaround.

  Further Problem Description: The following LOG messages and errors are found:

```
Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed -Traceback=
604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z Mar
30 01:27:38.447: %LICENSE-2-VLS_ERROR: 'VLSsetInstallLicenseStorage' failed with an
error - rc = 136 - 'Error[136]: Specified license store doesn't exists.' -Traceback=
604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z
```

- CSCtq28732

  Symptoms: Memory leak observed when device configured with the **parameter-map type inspect global** command.

  Conditions: Device is configured with the **parameter-map type inspect global** command.

  See also Cisco Security Advisory: Cisco IOS Software IPS and Zone Based Firewall Vulnerabilities, at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw

Workaround: None.

Further Problem Description: The following software table provides the first fixed release for each affected train for this specific Cisco ID.

+----------+ | Release | First Fixed Release for this | | | Cisco bug ID | +---------+----------+ | 15.0 Releases | +---------+----------+ | No affected 15.0 releases | +---------+----------+ | 15.1 Releases | +---------+----------+ | 15.1M | 15.1(4)M2 | | 15.1MR | Not Vulnerable | | 15.1S | Not Vulnerable | | 15.1SG | Not Vulnerable | | 15.1T | 15.1(2)T4, 15.1(3)T | | 15.1EY | Not Vulnerable | | 15.1GC | Vulnerable | | 15.1MWR | Not Vulnerable | | 15.1XB | Vulnerable | +---------+----------+ | 15.2 Releases | +---------+----------+ | No affected 15.2 releases | +---------+----------+

- CSCtq30875

  Symptoms: A Cisco ISR G1 will display “March 11, 2011” when the **show clock** command is entered. This will effect functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

  Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

  Workaround: The clock can be set manually via CLI.

- CSCtq36153

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCtq39406

  Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

  Conditions: This symptom occurs when you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM.

  Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- CSCtq47428

  Symptoms: A Cisco router acting as an SRST may unexpectedly reload due to a bus error.

  Conditions: This symptom is observed with phones registered to the SRST.

Workaround: There is no workaround.

- CSCtq56727

  Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash.

  The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP, and other processes.

  “sh proc mem sorted” shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

  Conditions: This symptom occurs when the SIP trunk in Unified Communications Manager pointing to the gateway is configured with a DTMF signaling type of “no preference” and the SIP gateway is configured with DTMF relay as sip- kpml.

  Workaround: There are two workarounds:

  1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
  2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”

  Recovery: In order to recover from the crash, you must reload the gateway router.

- CSCtq61850

  Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

  Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

  Workaround: There is no workaround.

- CSCtq64951

  Symptoms: The following message is displayed:

  ```
  %CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality
  with securityk9 technology package license.
  ```

  The **show platform cerm** command output shows all tunnels in use by SSLVPN.

  ```
  Number of tunnels 225 ... SSLVPN D D 225 N/A
  ```

  The **show webvpn session context all** command output shows no or very few active sessions.

  ```
  WebVPN context name: SSL_Context

  Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
  ```

  Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

  Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq75008

  Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

  Conditions:

  – The Cisco 7206 VXR works as a server for L2TP over IPsec.
  – Encryption is done using C7200-VSA.
  – More than two clients are connected.

  If client sessions are kept up for about a day, the router crashes.

Workaround: There is no workaround.

- CSCtq83629

  Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

  Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

  Workaround: Line card reload is required to resolve the problem.

- CSCtq86500

  Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

  Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

  Workaround: Disable VSA and use software encryption.

- CSCtq86515

  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq91176

  Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.

  Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

  Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

  Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtr04829

  Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

  Conditions: This symptom occurs when the hardware address is zero.

  Workaround: There is no workaround.

- CSCtr11620

  Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

  Conditions: This symptom is observed when a Cisco 2911 is used.

  Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr29338

  Symptoms: A router crashes.

  Conditions: The symptom is observed after an "%ISDN-6-DISCONNECT" message from "unknown" followed by a couple of "Illegal Access to Low Address" messages.

  Workaround: There is no workaround.

- CSCtr44686

  Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

```
policy-map type inspect smtp SMTP_L7_P1
  class type inspect smtp SMTP_L7_C1
    reset
policy-map type inspect smtp SMTP_L7_P2
  class type inspect smtp SMTP_L7_C2A
    reset
  class type inspect smtp SMTP_L7_C2B
    reset
```

  Conditions: The symptom is observed with the above maps.

  Workaround: Replace "reset" with "log".

- CSCtr46123

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

  Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y
  ipv6 enable
```

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z
  no ipv6 address
  ipv6 address ...
```

- CSCtr54269

  Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.

  Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.

  Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- CSCtr86437

  Symptoms: NAT-PT function does not work properly after an interface flap occurs.

  Conditions: The symptom is observed when you configure NAT-PT on the router.

  Workaround: Reconfigure “ipv6 nat prefix.”

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCtr97640

  Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

  Conditions: None.

  Workaround: None—Physically securing the router is important.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.9/1.8:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C CVE ID CVE-2011-3289

  has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts28315

  Symptoms: A DHCP PD request does not accept a specific server.

  Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:

  http://tools.ietf.org/html/rfc3633#section-10

  A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.

  Workaround: There is no workaround.

- CSCts33952

  Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

  Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.

  Workaround: There is no workaround.

- CSCts59014

  Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

  Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

  Workaround: There is no workaround.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey, when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCtt20215

  Symptoms: VWIC3 E1 cas connect to PBX, controller down after reload

  Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

  Workaround: Need to unplug/plug the cable, or reset link from PBX side, controller will come up.

Resolved Caveats—Cisco IOS Release 15.1(1)T3

Cisco IOS Release 15.1(1)T3 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T3 but may be open in previous Cisco IOS releases.

- CSCsk65515

  Symptoms: Spurious or misaligned memory access can be seen at atm_nvgen_static_map.

  Conditions: The symptoms can be observed when an SVC is configured on an ATM interface and when executing the command **show running- config**.

  Workaround: There is no workaround.

- CSCso33003

  Symptoms: If a child policy is attached to a parent policy twice, the router will reload if child policy configuration is removed.

  Conditions: The parent policy needs to be attached to target interface.

  Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCta26520

  Symptoms: The following traceback is seen:

  ```
  %IDBINDEX_SYNC-3-IDBINDEX_LINK: Driver for IDB type 0 changed the Identity of
  interface "Tunnel1" without deleting the old Identity first.
  ```

  Conditions: This symptom is observed when numerous tunnel interfaces are rapidly added and removed.

  Workaround: There is no workaround

- CSCtb07984

  Symptoms: A Cisco ASR router acting as LNS fails to apply D2 QoS on first few sessions after every new reboot and configures the D2 QoS on all subsequent sessions.

  Conditions: The symptom is observed when multiple routes exist on an LNS router to reach LAC router. PPPoX sessions are brought on LNS with D2 QoS model after new reboot of router.

  Workaround 1: LNS router configures D2 QoS on all subsequent sessions in Cisco IOS Release 12.2XND images.

  Workaround 2: In Cisco IOS Release 12.2XNE images, LNS router should have a single route to reach LAC router.

  Workaround 3: Wait until CEF is converged before bringing up a second session on the LNS router.

- CSCtc67457

  Symptom: Cisco ASR1000-RP2 crash is seen with the IKMP process.

  Conditions: This symptom occurs with GetVPN group member configurations with VRF-lite.

  Workaround: There is no workaround.

- CSCtd10712

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCte18124

  Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024”.

  Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.

  Workaround: Create ATM PVC without “atm vc-per-vp 1024”.

- CSCte78406

  Symptoms: The following error message is logged at the new standby RP when PTA sessions are established:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-Access2.1
  linked to wrong idb Virtual-Access2.1
  ```

  Conditions: The symptom is observed when PTA sessions are established, then an RP switchover is performed. After both RPs sync up, flap the sessions. The error messages are logged at the new standby RP.

  Workaround: There is no workaround.

- CSCtf26639

  Symptoms: A router crashes when turning on WAAS, adding a couple of specific class maps, and then turning off WAAS.

  Conditions: This is a corner case that is seen only when a specific type of filter is used with two or more classes; for example, for a WAAS class of the following type:

  ```
  class-map type waas DT-40 match tcp source ip 192.168.1.116 dest port 10040 10049
  class-map type waas DT-50 match tcp source ip 192.168.1.116 dest ip 192.168.101.117
  port 10050 10059
  ```

  ```
  policy-map type waas waas_global class DT-40 insert-before waas-default optimize tfo
  application DT-40 class DT-50 insert-before waas-default optimize tfo application
  DT-50 end
  ```

  The router will crash with such a configuration. Here, we have all TCP filters with same source IP address. This is the special condition.

  Workaround: There is no workaround.

- CSCtf36402

  Symptoms: A Cisco router crashes when the user telnets and Transmission Control Block is cleared for that session before entering the password.

  Conditions: This symptom is observed when aaa authentication protocol is set to TACACS.

Workaround: Do not clear the Transmission Control Block for a session before entering the password.

- CSCtf56107

  Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

  Conditions: The symptom is observed when an unknown notify message is received.

  Workaround: There is no workaround.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCth20696

  Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

  Conditions: The symptom is observed with Cisco IOS Release 12.4(25c).

  Workaround: There is no workaround.

- CSCth35515

  Symptoms: Linecard crash could occur on an SSO when a router runs MPLS.

  Conditions: This symptom may occur when multiple back-to-back switchovers occur.

  Workaround: There is no workaround.

- CSCth40506

  Symptom: A Cisco voice gateway does not have its GigabitEthernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

  Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

  Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

  ```
  -- Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0 --
  ```

  Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

  ```
  -- .May 4 17:49:29.120 GMT=+1: ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry:
  Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
  ```

  The call, however, is not cleared from the PRI.

- CSCth46888

  Symptoms: When the ARP entry is refreshed due to timeout or use of the **clear arp** command, the router sends ARP request for cached MAC address. However, the request message does not use virtual MAC for Source (Sender) MAC.

  Conditions: The symptom is observed when the router is VRRP master and VRRP IP is configured the same as the interface IP.

  Workaround: There is no workaround.

- CSCth57478

  Symptoms: When configuring SIP digest authentication, user names with more than 25 characters are truncated in the running config and cause the password component to be corrupted. This error is saved through to startup configuration, causing the authentication to be lost on reboot.

  Conditions: This symptom is observed with a normal dial-peer configuration on a POTS dial-peer running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCth69364

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

- CSCth93218

  Symptoms: The error message `"%OER_BR-4-WARNING: No sequence available"` displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCth94814

  Symptoms: Crash is seen in static route component.

  Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.

  Workaround: There is no workaround.

- CSCti05663

  Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

  Conditions: The symptom is observed in the case of an numbered relay.

  Workaround: There is no workaround.

- CSCti07805

  Symptoms: Router reloads @sipSPIUpdSrtpSession.

  Conditions: This symptom is observed during Hold/Resume on a basic SRTP call with Cisco IOS Release 15.1(2.3)T.

  Workaround: There is no workaround.

- CSCti39902

  Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

  Conditions: This symptom is observed when RRI is configured on the UUT .

  Workaround: There is no workaround.

- CSCti50607

  Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

  Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

  Workaround: There is no workaround.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: This symptom is observed when ALL of the following conditions are met:

  – The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”

  – It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload

  – When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages

  – Both peers must be multisession-capable

  – “Transport multi-session” must not be configured on either device, or enabled by default on either device

  – “Graceful restart” must not be configured.

  Workarounds:

  1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
  2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
  4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
  5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

  Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS 12.2(33)SB-based releases if the 12.2(33)SB router is the one not reloading.

- CSCti61949

  Symptoms: Unexpected reload with a `"SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header"` and `"chunk name is BGP (3) update"` messages.

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

  Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67447

  Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

  Conditions: The symptom is observed under the following conditions:

  1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2
  2. Enable MPLS LDP GR.

  Workaround: There is no workaround.

- CSCti68721

  Symptoms: The output of **show performance monitor history interval <all | given #>** will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti71071

  Symptoms: The command **show policy-map multipoint** does not show any output on a hub, configured with a per-tunnel-QoS policy on its tunnel interface. The command is also not displayed in the parser options upon issuing **show policy-map ?**.

  Conditions: The symptom is observed with the **show policy-map multipoint** command.

  Workaround: There is no workaround.

- CSCti75666

  Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.

Workaround: Convert H.323 leg to SIP.

- CSCti79848

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

  - Memory leak in Cisco IOS Software
  - Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw.

- CSCti84762

  Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

  Conditions: This is seen with peer flaps or route churn and with an interface flap.

  Workaround: Do a hard reset of the stuck peers.

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface)
  3. Change the configuration in such a way that nexthop is reachable
  4. Configure a new static route through the same nexthop IP address used in step 1.

  Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti87502

  Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.

  Conditions: This symptom is observed when attempting to launch CP Express.

  Workaround: A power cycle fixes the issue temporarily.

- CSCti90602

  Symptoms: The PPTP connection is not established when “ip nat outside” is configured on the NAT router. The NAT router is between the client and the server.

  Conditions: This symptom is observed only with the PPTP connection; all other traffic works fine.

  Workaround: There is no workaround.

- CSCti96028

  Symptoms: A build failure is seen due to the fix committed using CSCti67511 (“Borghetti DSL PHY Firmware upgrade through usb flash”).

  Conditions: This symptom is observed when building Cisco 180x platform IOS images.

  Workaround: There is no workaround.

- CSCti98219

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj08533

  Symptoms: QoS classification fails on egress PE if the route is learned via BGP.

  Conditions: The symptom is observed when there are redundant paths to the CPE.

  Workaround: Use only one path between PE and CPE.

- CSCtj20545

  Symptoms: When a host behind a ZBF implementation is disconnecting ungracefully and loses the TCP connection information, TCP keepalive sessions will only be terminated on the other endpoint after the TCP keepalive times out. This is because the RST from the host, in response to the keepalive from other endpoint, is out-or-order and gets dropped by the ZBF.

  Conditions: The symptom is observed when you have TCP connections using keepalive (keepalive with both sequence number and acknowledgment number one less than expected for a session) going over a ZBF implementation.

  Workaround: Shorten the keepalive timeout on the other endpoint.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

  ```
  Router1#sho inv NAME: “chassis”, DESCR: “2801 chassis” PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF

  NAME: “motherboard”, DESCR: “C2801 Motherboard with 2 Fast Ethernet” PID: CISCO2801 , VID: V04 , SN: FOC11456KMY

  NAME: “VIC 0", DESCR: “2nd generation two port EM voice interface daughtercard” PID: VIC2-2E/M= , VID: V , SN: FOC081724XB

  NAME: "WIC/VIC/HWIC 1", DESCR: “4 Port FE Switch” PID: HWIC-4ESW , VID: V01 , SN: FOC11223LMB

  NAME: “WIC/VIC/HWIC 3", DESCR: “WAN Interface Card - DSU 56K 4 wire” PID: WIC-1DSU-56K4= , VID: 1.0, SN: 33187011

  NAME: “PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capcity” PID: PVDM2-8 , VID: NA , SN: FOC09123CTB
  ```

Workaround: Do a shut/no shut on the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is entered:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
  chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP Scanner", ipl= 0, pid= 549
  with call stack 0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
  0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
  0x403A4E84:bgp_scanner(0x403a4c50)+0x234
  ```

  Conditions: This symptom is rarely observed, but it can be seen when **clear ip bgp *** is entered with a lot of routes and route-map-cache entries.

  ```
  Router# show ip bgp sum

  BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
  main routing table version 1228001 604000 network entries using 106304000 bytes of
  memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
  attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
  of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
  cache entries using 4565920 bytes of memory
  ```

  The **clear ip bgp *** command is not a very common operation in production network.

  Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the symptom will not be observed.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an "Exit Mismatch" message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

  Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

  Workaround: There is no workaround.

- CSCtj30155

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCtj35792

  Symptoms: The onboard GE on a Cisco 3900 (driver PQ3_TSEC) with "media-type sfp" goes to 1000/HD when it is connected by fiber to a gig port that is not doing autonegotiation.

  Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation. The Cisco 3945-E does not have this problem.

  Workaround: Configure autonegotiation on the other side, if possible.

Further Problem Description: It is impossible to disable autonegotiation on the Cisco 3900 because of CSCth72105.

- CSCtj41194

  Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6.

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

  Workaround: There is no workaround.

- CSCtj48629

  Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj48913

  Symptoms: Track does not recognize when an HTTP IP SLA probe’s status changes to OK.

  Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

  Workaround: There is no workaround.

- CSCtj53363

  Symptoms: Router hangs and console does not respond indefinitely.

  Conditions: The symptom is observed with the following conditions:

  - AIM-VPN in ISR + ZBFW; or
  - A Cisco 2811/2821 Onboard VPN + ZBFW
  - Once traffic starts, router hangs within minutes.

  Workaround: If running a Cisco 2811/2821, use sw crypto + ZBFW.

  Alternate Workaround: If running with a Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

  Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

  Workaround: There is no workaround.

- CSCtj77477

  Symptom: High delay in priority queue when using CBWFQ/LLQ. For example:

  ```
  EFM rate 2304 kbps
  888E Average delay: 42ms 888E Max delay: 63ms HWIC-4SHDSL-E Average delay: 216ms
  HWIC-4SHDSL-E Max delay: 361ms
  ```

  Conditions: The symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E.

  Workaround: Configure hierarchical QoS on WAN G.SHDSL EFM interface.

  For example:

  ```
  EFM rate 2304 kbps
  policy-map CHILD class voice priority percent 25 class business bandwidth percent 50
  policy-map PARENT class class-default shape average 2100000 8400 0 service-policy
  CHILD
  ```

- CSCtj78210

  Symptoms: One-way audio. Moves from one port to another when the router is rebooted.

  Conditions: The symptom is observed when using multiple “session protocol multicast,” “connection trunk” configurations for LMR, E&M Immediate, and/or other multicast applications, such as the conditions where this was first detected, in a Radio over IP solution. Only affects PVDM3.

  Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

  For example, configure:

  ```
  voice-card 0 (1... 2... etc...) dspfarm dsp service dspfarm
  dspfarm profile x conf max sessions xx << use the maximum max partic << use the maximum
  associate app sccp no shutdown
  dspfarm profile x2 conf max sessions xx << use the maximum max partic << use the
  maximum associate app sccp no shutdown
  dspfarm profile x3 conf max sessions xx << use maximum (if allowed) max partic << use
  the maximum (if allowed) associate app sccp no shutdown
  dspfarm profile x conf shutdown no dspfarm profile x conf
  ```

  The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

  This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- CSCtj81533

  Symptoms: The following error messages is seen:

  ```
  np_vsmgr_modify_connection: invalid service id 11 passed
  ```

  No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

  Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

  Workaround: There is no workaround.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

Conditions: This issue occurs when summary address is advertised as follows:

```
ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
```

Workaround: There is no workaround.

- CSCtj84901

  Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

  Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

  1. Service Ready Engine modules (ISM and SM SRE)
  2. Etherswitch modules (SM and EHWIC)

  If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

  This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

  Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

  For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

  Conditions: The symptom is observed when the LAC router receives an incorrect `"Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID"` message from the multihop peer.

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

  Conditions: Testbed setup:

  1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured
  2. Use IXIA to generate 1Gbps traffic
  3. Wait until all the SAs have been established and traffic is stable
  4. Use CLI **clear crypto session** on EzVPN simulator.

  Workaround: There is no workaround.

- CSCtj94617

  Symptoms: Memory leak is seen while issuing the **show running** or the **show ip access-lists** command even though we do not have any named ACL configured on the box.

  Conditions: This symptom is observed when issuing the **show running** command.

  Workaround: There is no workaround.

Further Problem Description: The memory leak is in dynamic list that was created, which is not destroyed properly.

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown. See Further Problem Description below.

  Workaround: There is no workaround. Only a power cycle can remove the symptom.

  Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

  Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

  Workaround: There is no workaround.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, Release 15.1 (2)T and Release 15.1(01)S and with the following configurations:

  ```
  Router 1: interface Ethernet0/0 ip address 10.0.12.1 255.255.255.0 !

  interface Ethernet1/0 ip address 10.0.120.1 255.255.255.0 ! router bgp 100 no
  synchronization bgp log-neighbor-changes neighbor 172.16.0.1 remote-as 200 neighbor
  172.16.0.1 ebgp-multihop 255 no auto-summary !

  ip route 0.0.0.0 0.0.0.0 10.10.200.1 ip route 172.16.0.1 255.255.255.255 10.0.12.2 ip
  route 172.16.0.1 255.255.255.255 10.0.120.2

  Router 2: interface Loopback200 ip address 10.10.200.1 255.255.255.0 ! interface
  Loopback201 ip address 172.16.0.1 255.255.255.0 ! interface Ethernet0/0 ip address
  10.0.12.2 255.255.255.0 !

  interface Ethernet1/0 ip address 10.0.120.2 255.255.255.0 ! router bgp 200 no
  synchronization bgp log-neighbor-changes network 10.10.200.0 neighbor 10.0.12.1
  remote-as 100 neighbor 10.0.12.1 update-source Loopback201 no auto-summary ! ip route
  0.0.0.0 0.0.0.0 10.0.12.1 !
  ```

  Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes.”

- CSCtk12681

  Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

  Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk47891

  Symptoms: Traffic might be blackholed when LC is reset, if Fast Reroute (FRR) is in use.

  Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk53130

  Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

  ```
  Incompatible with ipv6 command on Vp1 - command rejected.
  ```

  Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

  Workaround: There is no workaround.

- CSCtk53534

  Symptoms: Router crashes.

  Conditions: The symptom is observed with some combination of zone-based firewall and policy configuration and with IPv6 traffic.

  Workaround: Disable global parameter-map.

- CSCtk56570

  Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.

  Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

  Workaround: Disable media transcoder-high-density.

- CSCtk62247

  Symptoms: IKEv2 session fails to come up with RSA sign authentication.

  Conditions: The symptom is observed with a hierarchical CA server structure.

  Workaround: Use non-hierarchical CA servers.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla.

- CSCtk68647

  Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

  Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

  Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to re-sync after the server clock changes its time and after the NTP falls back to the local clock.

  Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

Workaround: There is no workaround.

- CSCtk84116

  Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

  Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

  Workaround: There is no workaround.

- CSCtk95992

  Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

  Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

  Workaround: Configure the command **dlsw udp-disable**.

  Further Problem Description: This symptom occurs in the following (and later) releases:

  Cisco IOS Release 12.4(15)T14, Release 12.4(24)T4, Release 15.0(1)M3, Release 15.1(1)S, Release 15.1(2)T, Release 12.2(33)SXI4, and Release 12.2(33)SXI4a.

- CSCtl00467

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed when call monitoring is enabled and the “conference call” feature is used.

  Workaround: There is no workaround.

- CSCtl04285

  Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

  Conditions: The symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are Cisco IOS Release 12.2(33)SRE, Release 15.0M, and 12.2(33)XNE and later releases.

  Workaround: There is no workaround.

- CSCtl05684

  Symptoms: Xauth user information remains in “show crypto session summary” output.

  Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different username during P1 rekey.

  Workaround: Use save-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- CSCtl21695

  Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million . **Debug vpdn l2x ev/er** shows:

  ```
  PPTP _____:________: TCP connect reqd from 0.0.0.0:49257 PPTP _____:________: PPTP,
  no cc in l2x
  ```

Conditions: This symptom occurs when LNS is configured for PPTP aggregation and over one millions tunnels have been accepted (on VPDN level).

Workaround: Reload LNS.

- CSCtl47666

  Symptom: Intermittent call drops for CME SNR calls that go to voicemail.

  Conditions: This symptom is observed on a Cisco IP phone with SNR configured. When the “no answer” timer is reached, the call will intermittently drop instead of going to voicemail.

  Workaround: There is no workaround.

- CSCtl57055

  Symptoms: A router may unexpectedly reload when the rttMonStatsTotalsEntry MIB is polled by SNMP.

  Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release, is configured for SNMP polling, and when the rttMonStatsTotalsEntry is polled with an IP SLA probe configured.

  Workaround: Configure NMS to stop polling the rttMonStatsTotalsEntry or create a view and block the MIB on the router.

  Alternate Workaround: Since the issue affects only Cisco IOS 15.1T releases, use a Cisco IOS Release 15.0(1)M or earlier rebuild.

- CSCtl71478

  Symptoms: In an HA system, the following error message is displayed on the standby RP and LC:

  ```
  “OCE-DFC4-3-GENERAL: MPLS lookup unexpected”
  ```

  Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

  Workaround: There is no workaround.

- CSCtl73914

  Symptoms: A Cisco 2921 Gateway that is running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

  Conditions: The symptom is observed if the P-Associated-URI of the 200 Ok response contains any special characters (!*.!) in Tel URI Parsing.

  Workaround: There is no workaround.

- CSCtl77735

  Symptoms: Saving a configuration to NVRAM may fail.

  Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

  Workaround: Erasing the startup configuration and saving again may recover the configuration.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtl98270

  Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

  Conditions: The symptom is observed in Cisco IOS Release 15.1(2)T2 and later releases.

  Workaround: Execute a shut/no shut to fix the issue.

- CSCtn26785

  Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

  ```
  3845#sh int atm 1/0 stat ATM1/0 Switching path Pkts In Chars In Pkts Out Chars Out
  Processor 98170 10995040 1 68 Route cache 0 0 98170 10995040 Total 98170 10995040
  98171 10995108 3845#
  ```

  ```
  3845#sh cef int atm 1/0 ATM1/0 is up (if_number 5) Corresponding hwidb fast_if_number
  5 Corresponding hwidb firstsw->if_number 5 Internet address is 64.65.248.174/30 ICMP
  redirects are never sent Per packet load-sharing is disabled IP unicast RPF check is
  disabled Input features: Ingress-NetFlow Output features: Post-Ingress-NetFlow IP
  policy routing is disabled BGP based policy accounting on input is disabled BGP based
  policy accounting on output is disabled Hardware idb is ATM1/0 Fast switching type 9,
  interface type 138 IP CEF switching enabled IP CEF switching turbo vector IP prefix
  lookup IPv4 mtrie 8-8-8-8 optimized Input fast flags 0x0, Output fast flags 0x0
  ifindex 5(5) Slot Slot unit 0 VC -1 IP MTU 4470 3845#
  ```

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn27599

  Symptoms: The OIR of NM-1T3/E3 line card crashes the router.

  Conditions: This symptom is observed only on the Cisco 3945 router.

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is seen in EzVPN process.

  Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

  Workaround: There is no workaround.

- CSCtn77154

  Symptoms: The Stateful Inspection Feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets being punted to the CPU. This causes overall performance degradation.

  Conditions: This symptom is observed when two outside NAT interfaces are configured and “no ip nat service nbar” is configured on the interface.

  Workaround: Configure “ip nbar protocol discovery” on the interface.

- CSCtn87012

  Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

  Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

  Workaround: Pick up the phone during the ringing OFF cycle.

- CSCto23807

  Symptoms: A Cisco device crashes when trying to transfer a call.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T2.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(1)T2

Cisco IOS Release 15.1(1)T2 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T2 but may be open in previous Cisco IOS releases.

- CSCso02147

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCsu95339

  Symptoms: Output from the **show idmgr session** command displays a corrupted service name.

  Conditions: Enter the **show idmgr session** command.

  Workaround: There is no workaround.

- CSCsz69148

  Symptoms: When running an Embedded Syslog Manager (ESM) TCL script to filter logs on a Cisco ASR 1000 Series Aggregation Services router, memory leaks in IOSD ipc task and ESM Logger occur.

  Conditions: The symptom is observed with RP1 and RP2. Any feature which uses heavy logging (for example, audit logging for firewall features) will encounter this issue readily (the trigger is the rate of logging rather than the volume of log messages).

  Workaround: There is no workaround.

  Further Problem Description: The IOSD ipc task and ESM logger consume more and more memory until there is no more free memory available on the router. You can track the memory consumption with the **show processor memory sort** command and monitor the amount of memory the IOSD ipc task and ESM logger consume over time.

  An example configuration:

  ```
  logging buffered filtered
  logging filter harddisk:ESMscript.tcl
  ```

- CSCta15808

  Symptoms: Router crashes while printing traceback.

Conditions: The symptom is observed while printing traceback.

Workaround: There is no workaround.

- CSCta53372

  Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

  Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

  Workaround: Reset the RRI session.

- CSCtb55576

  Symptoms: When an HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

  Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

  Workaround: There is no workaround.

- CSCtc33679

  Symptoms: Routes are not being controlled properly when PIRO is used.

  Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

  Workaround: There is no workaround.

- CSCtc55897

  Symptoms: R2 will not advertise the routes.

  Conditions: The symptom is observed under the following conditions:

  1. R2 has two IBDG neighbors in the same update-group one neighbor with 4BAS and the other with 2BAS capability.
  2. The locally originated routes or routes without any AS_PATH will not be advertised to this kind of group.

  Workaround: Try to make the 2BAS and 4BAS neighbors fall into different update-groups by configuring dummy route-maps.

- CSCtd39579

  Symptoms: A router crashes when we try to remove service-policy/waas from an interface.

  Conditions: Traffic should be hitting the interface, CPU utilization should be high, and NAT should be applied on the interface as well.

  Workaround:

  1. Remove NAT from the interface.
  2. Remove the service policy.
  3. Re-apply NAT.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

  Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

  Workaround: There is no workaround.

- CSCte62190

  Symptoms: A router crashes when the RSA key is generated with redundancy option and then the RSA key pair is deleted using the **crypto pki zeroise** command. All other possible triggers are not known at this time.

  Conditions: Device running IOS and crypto.

  Workaround: There is no workaround.

- CSCte64544

  Symptoms: Calls fail following hook flash on a T1-CAS circuit.

  Conditions: The symptom is observed following outbound calls over a T1-CAS E&M, and after a hookflash.

  Workaround 1: Reorder circuits in CUCM RG.

  Workaround 2: Perform a shut/no shut on the T1-CAS controller.

- CSCte92581

  Symptoms: A VRF becomes stuck during deletion in a rear condition (not something that is seen every time).

  Conditions: This symptom is observed when the **no ip vrf** command is entered.

  Workaround: There is no workaround.

  Further Problem Description: The stuck VRF cannot be reused.

- CSCte94301

  Symptoms: IPv6 PBR is not applied to locally-originated ping packets.

  Conditions: This symptom occurs when IPv6 PBR is configured for application to locally-originated ping packets.

  Workaround: There is no workaround.

- CSCte98702

  Symptoms: When using NAT, "%SYS-3-INVMEMINT and %SYS-2-MALLOCFAIL" are printed to the console and no traffic passes.

  Conditions: The symptom is observed when NAT is configured.

  Workaround: There is no workaround.

- CSCtf34720

  Symptoms: DR will not send a periodic join for an SSM group with a "static- group" configuration on the RPF interface. This will result in the S,G states expiring in the upstream routers and may result in traffic loss.

  Conditions: The symptom is observed when the static-group join is configured on the RPF interfaces and the output interface list of the mroute is NULL.

  Workaround: Add a local join by using **ip igmp join-group** for the same group and source, so that it adds a local interested receiver and sends a periodic join upstream.

- CSCtf54561

  Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf** *vrf-name* command is issued.

  Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

  Workaround: Command should not be issued when many topology changes occur on interface flaps.

- CSCtg25798

  Symptoms: The issue is associated with the two labels imposition for the next-hop address. If there is no label bind for the destination prefix and in order to reach next-hop address the router imposes two labels, only one label is imposed for the final prefix.

  Conditions: The symptom occurs when all of the following conditions are met:

  1. The prefix does not have a label bind (BGP prefixes for example).
  2. There is a static route for the next-hop address pointing to the tunnel only.
  3. The router imposes two labels for the next-hop address.

  Workaround: There are three potential workarounds:

  1. Explicit next hop avoiding recursive research: “ip route 192.168.4.4 255.255.255.255 Tu1 192.168.4.4” (i.e.: breaking rule 2).
  2. Use “neighbor 192.168.1.1 send-label” on both PEs (i.e.: breaking rule 1).
  3. Use “mpls traffic-eng signaling interpret explicit-null verbatim” on P (i.e.: breaking rule 3).

  Further Problem Description: In the following example 192.168.200.200 is the final destination. There is no label bind for this prefix and it is recursive to 192.168.100.100:

```
PE1# show mp ld bin 192.168.200.200 32
lib entry: 192.168.200.200/32, rev 35
         local binding:  label: 31
PE1# show ip route 192.168.200.200
Routing entry for 192.168.200.200/32
   Known via "static", distance 1, metric 0
   Routing Descriptor Blocks:
   * 192.168.100.100
       Route metric is 0, traffic share count is 1
```

  The next-hop 192.168.100.100 has a static route pointing to the tunnel and is double tagged:

```
PE1# show ip route 192.168.100.100
Routing entry for 192.168.100.100/32
   Known via "static", distance 1, metric 0 (connected)
   Routing Descriptor Blocks:
   * directly connected, via Tunnel10
       Route metric is 0, traffic share count is 1
PE1# show ip cef 192.168.100.100
192.168.100.100/32
   attached to Tunnel10 label 26
PE1# show mp ld bin 192.168.100.100 32
lib entry: 192.168.100.100/32, rev 30
         local binding:  label: 29
```

```
        remote binding: lsr: 192.168.2.2:0, label: 26
        remote binding: lsr: 192.168.4.4:0, label: 26 <<<<< tunnel head-end.
```

So the traffic to 192.168.200.200 should also be double tagged as shown below:

```
PE1# show ip cef 192.168.200.200
192.168.200.200/32
   nexthop 192.168.100.100 Tunnel10 label 26
```

However traffic is leaving the router only with the tunnel label:

```
PE1# trace 192.168.200.200
Type escape sequence to abort.
 Tracing the route to 192.168.200.200
   1 192.168.12.2 [MPLS: Label 20 Exp 0] 4 msec 0 msec 0 msec
   2 192.168.23.3 [MPLS: Label 23 Exp 0] 4 msec 0 msec 0 msec
   3 192.168.34.4 4 msec 0 msec 0 msec
   4 192.168.48.8 4 msec *  4 msec
```

- CSCtg42904

  Symptoms: Router crashes with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address after applying the flow monitor to
  virtual-template interface
  ```

  Conditions The symptom is observed on a router configured with EasyVPN.

  Workaround: There is no workaround.

- CSCtg51476

  Symptoms: Cisco ISR G2 routers reload on their own with a bus error.

  Conditions: This symptom is observed when BFD is configured.

  Workaround: Remove BFD.

- CSCtg57831

  Symptoms: In the event of a failover, there is a serial number mismatch on the active and standby.

  Conditions: The symptom is observed in an High Availability CA servers environment, using Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtg58786

  Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

  Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

  Workaround: There is no workaround.

- CSCtg63096

  Symptoms: The **deny ip any any fragments** command shows a high number of hits for traffic that may not be truly fragmented.

  Conditions: This symptom occurs when “deny ip any any fragments” may be configured at the top of the ACL.

  Workaround: There is no workaround.

- CSCtg71332

  Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

  Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

  Workaround:

  1. Use SP services feature set.
  2. Upgrade router to Cisco IOS Release 12.4(24)T.
  3. Install one or more PVDM sLOTS.

- CSCtg91201

  Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

  Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

  Workaround: There is no workaround.

- CSCtg91336

  Symptoms: A Cisco router may crash during show command **show ip ospf rib** execution.

  Conditions: This symptom is observed in Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

  – A user enters the **show ip ospf rib** command and stops in the middle.
  – The OSPF local rib is significantly changed; for example, routes are removed.
  – A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

  Workaround: Do not enter the **show ip ospf rib** command. If it is necessary to use the command, enter **terminal length 0** and print the entire output.

- CSCtg92783

  Symptoms: Uplink performance degrades by about 70% with HWIC-3G-CDMA when bound to external dialer interface when compared to using cellular interface legacy DDR.

  Conditions: This symptom is seen on live network when performance is measured using latency sensitive Internet speed test application.

  Workaround: Use cellular interface without binding to external dialer.

- CSCtg94250

  Symptoms: Removing **address-family ipv4 vrf** *vrf* (in router BGP) followed by **no ip vrf** *vrf* (where "vrf" is the same) could result in a crash.

  Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

  1. **no address-family ipv4 vrf** *vrf*
  2. **no ip vrf** *vrf*
  3. **ip vrf** *vrf*

  The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).
2. Give sufficient time for (1) to complete before applying (2).

- CSCtg95940

  Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

  Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

  Workaround: There is no workaround.

  Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCth06812

  Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

  Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1 (XNE1) and the following configuration:

```
R1(config)# parser view SUPPORT
R1(config-view)# secret cisco
R1(config-view)# commands exec include ping
R1(config-view)# commands exec include configure terminal
R1(config-view)# commands exec include show ip ospf neighbor <--Where we see the hang.
```

  Workaround: Do not configure “commands exec include show ip ospf neighbor” command in parser view configuration.

- CSCth15268

  Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.

  Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit on.

  Workaround: Set “llc2 local-window” to 1.

- CSCth16011

  Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

  Conditions: Introduce loss to network.

  Workaround: There is no workaround.

- CSCth29426

  Symptoms: When you issue a **reload** command with a getmany looping on ciscoFlashMIB, the router hangs.

  Conditions: The symptom is observed when a getmany is running with only one router. The chances of hitting the issue seem to be increased if a **write memory** has been done before reload or even if the configuration is dirty and you respond “no” to the save configuration prompt.

  Workaround: Avoid reloading while doing an SNMP walk on ciscoFlashMIB.

- CSCth31395

  Symptoms: A Frame Relay PVC stays in the INACTIVE state.

Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

Workaround: There is no workaround.

- CSCth33457

  Symptoms: A Cisco IOS router configured with IPSec (IP Security) may reload when receiving encrypted packets.

  Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

  - ip accounting precedence input
  - ip accounting mac-address input
  - WCCP
  - Flexible NetFlow
  - BGP accounting
  - uRPF
  - mpls accounting experimental input

  Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth33500

  Symptoms: NAS port is reported as zero on LNS.

  Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

  Workaround: There is no workaround.

- CSCth36114

  Symptoms: A crash is seen after executing the **write memory** command via SDM.

  Conditions: The symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

  Workaround: Use Cisco IOS 12.4 versions.

- CSCth36740

  Symptoms: A router may experience CRC and Runt errors.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2 and when the on-board GigabitEthernet interface is hard-coded to 10mb/full duplex. It is seen with the following routers: Cisco 1900 series, Cisco 2900 series, and Cisco 3900 series.

  Workaround: There is no workaround.

- CSCth37092

  Symptoms: A crash is observed in the PKI-HA feature when the standby tries to sync up with the active router.

  Conditions: When the PKI server is created on the active router with a “database archive password” configuration, the PKI server is cloned on the standby. Soon after, the active router crashes.

  Workaround: There is no workaround.

- CSCth38699

  Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-Group mappings.

- CSCth45413

  Symptoms: The environmental alarm has additional hard disk drive information in the Syslog message.

  Conditions: The symptom is observed when there is one of the following service modules in the system:

  - SM-SRE-900-K9
  - SM-SRE-700-K9
  - NME-APPRE-522-K9
  - NME-APPRE-502-K9
  - NME-APPRE-302-K9
  - NME-WAE-502-K9
  - NME-NAM-120S
  - NME-NAM-80S
  - NME-NAC-K9
  - NME-CUE
  - NME-UMG-EC
  - NME-UMG

  Workaround: There is no workaround.

- CSCth49421

  Symptoms: Transparent bridging stops working.

  Conditions: The symptom is observed when the interface goes to standby from active. The output of **show controllers gigabitethernet** *slot/port* shows these fields (at the end of output):

  When working:

```
Software filtered frames: 0
    Unicast overflow mode: 1 <--
    Multicast overflow mode: 1
    Promiscuous mode: 1
    Total Number of CAM entries: 8
  Port Stopped: N
```

  When not working:

```
Software filtered frames: 0
    Unicast overflow mode: 0 <--
    Multicast overflow mode: 1
    Promiscuous mode: 1
    Total Number of CAM entries: 4
```

```
  Port Stopped: N
```

Workaround: Remove bridging and reconfigure it on the interface.

- CSCth58283

  Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

  Conditions: NAT is enabled.

  Workaround: There is no workaround.

- CSCth62854

  Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

  Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

  Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

  Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

  Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

  Workaround: There is no workaround.

- CSCth64271

  Symptoms: Routers in redundant configuration end up in Manual Swact = disabled.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCth65072

  Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

  Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

  Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth69361

  Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.

  Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.

  Workaround: There is no workaround.

- CSCth77531

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU in the BGP-related processes for several hours (greater than 2.5).

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process takes the most CPU; also, the number of routemap-cache entries should be very high.

```
Router# show ip bgp sum
BGP router identifier 1.1.1.1, local AS number 4739
```

```
BGP table version is 1228001, main routing table version 1228001 604000 network
entries using 106304000 bytes of memory
604000 path entries using 31408000 bytes of memory
762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results and the issue will not be observed.

- CSCth83508

  Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

  Conditions: The problem is seen when using WSMA to run the **session install** command.

  Workaround: Perform the install manually from a VTY session.

- CSCth84995

  Symptoms: Router may reload when performing an ISSU upgrade or downgrade.

  Conditions: This symptom occurs when performing an ISSU upgrade or downgrade.

  Workaround: There is no workaround.

- CSCth87587

  Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

  Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

  Workaround: There is no workaround.

  Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth87638

  Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

  Conditions: The symptom is observed on WIC-based platforms. It was seen originally on an Cisco IAD243x using a HWIC-CABLE-D-2.

  Workaround: Manually change the MAC address problem card.

  Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- CSCth97996

  Symptoms: A Cisco 39xx router may crash.

  Conditions: The symptom is observed during regular operations and with an extensive QoS configuration. The issue is seen when running Cisco IOS Release 15.0(1)M3.

  Workaround: There is no workaround.

- CSCth99237

  Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

Conditions: The symptom is observed under the following conditions:

1. If the client starts to send LCP echo requests during the PPP Authentication phase.
2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

Workaround: There is no workaround.

- CSCti08336

  Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

  Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are "IN" policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go "Out" of policy.

  Workaround: There is no workaround.

- CSCti10016

  Symptoms: After the **format** command is run on a 32GB or larger disk, the **show** command displays that only 4GB is free on the device.

  Conditions: The symptom is observed when formatting disk that is larger than 32GB in capacity.

  Workaround: Use a smaller size disk that has no more capacity than 32GB.

- CSCti10518

  Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

  Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

  Workaround: There is no workaround.

- CSCti13286

  Symptoms: Putting this configuration on a router:

```
router rip
  version 2
  no validate-update-source
  network 10.0.0.0
  no auto-summary
  !
  address-family ipv4 vrf test
   no validate-update-source
   network 172.16.0.0
   no auto-summary
   version 2
  exit-address-family
```

  and doing a reload causes the "no validate-update-source" statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti17190

  Symptoms: A router crashes when trying to do sre install.

  Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

  Workaround: There is no workaround.

- CSCti19627

  Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

  Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

  Workaround: Remove “call-park system application”.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti25280

  Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

  ```
  **ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
  ```

  Conditions: The symptom is observed when there is also a VWIC installed in the chassis (for example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

  Workaround: Remove the VWIC.

- CSCti26202

  Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

  Conditions: The symptom is observed on a Cisco 3900 series router.

  Workaround: There is no workaround.

- CSCti47649

  Symptoms: A router may crash with the message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04
  ```

Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

Workaround: There is no workaround.

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti55261

  Symptoms: On a phone button that has an overlay with call waiting DNs configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

  Conditions: The symptom is observed on a phone button that has an overlay with call waiting DNs and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti62226

  Symptoms: Voice port(s) that are created with PRI/ds0 configurations are active even after shutting down those ports. Because of this, unconfiguring PRI/ds0 configurations throws an error.

  Conditions: The symptoms are observed with Cisco IOS Release 15.0(1)M3 when shutting down the voice-port to unconfigure the controllers.

  Workaround: Do **no shut** first then **shut**.

  Further Problem Description: If you are running a script for regression which cannot be changed there is no workaround. If it is a user interactive case, the above workaround may help.

- CSCti72836

  Symptoms: The router crashes when removing an ACL.

  Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hashtable.

  Workaround: There is no workaround.

- CSCti75410

  Symptoms: A Cisco 887 voice gateway is unable to detect any interface.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCti86169

  Symptoms: A device that is acting as a DHCP relay or server crashes.

  Conditions: This symptom is observed when the **no service dhcp** command is configured.

  Workaround: There is no workaround.

- CSCti93398

  Symptoms: A Cisco 1861 router reloads.

  Conditions: The reload occurs upon booting.

Workaround: There is no workaround.

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07885

  Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

  Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

  Workaround:

  1. Configure CME-as-SRST with “srst mode auto-provision all”.
  2. Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:

     a) Stop the MIB on the NMS device that is doing the polling.

     b) Turn off SNMP polling on the device.

     c) Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1
   redistribute connected
   no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: This symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(1)T1

Cisco IOS Release 15.1(1)T1 is a rebuild release for Cisco IOS Release 15.1(1)T. The caveats in this section are resolved in Cisco IOS Release 15.1(1)T1 but may be open in previous Cisco IOS releases.

- CSCsl64247

  Symptoms: Router crashes 20-30 minutes after configuring “mode route control”.

Conditions: The symptom is observed when the router is configured as OER master.

Workaround: There is no workaround.

- CSCso20810

  Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. Occurs when multicast subsequently flows out a crypto-enabled interface.

  Conditions: This bug will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

  Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCsu31853

  Symptoms: TCP sessions in TIMEWAIT state cause buffer usage until they move to CLOSED state.

  Conditions: This symptom is observed with almost all TCP applications. It is mainly seen on low end switches.

  Workaround: There is no workaround.

- CSCsx56362

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

  Conditions: The symptom is observed when:

  1. BGP is configured.
  2. More than one equally-good route is available.
  3. BGP is configured to use less than the maximum available number of multipaths.

  Workaround: There is no workaround.

  Further Problem Description: The selection of non-oldest paths as multipaths is only problematic in releases which include CSCsk55120, because in such releases it causes changes with respect to whether paths are considered multipaths.

- CSCsz70049

  Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the telco side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.

  Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.

  Workaround: Issue the **clear interface bri** command to restore this state.

- CSCta58068

  Symptoms: During BGP convergence, a CPU spike may be seen on the local PE in an MVPN configuration.

  Conditions: The symptom may be observed with the following conditions:

  - Remote PE neighbor switchover.
  - On local PE, do a **clear ip bgp** *bgp nbr*.
  - On bringup of local PE.
  - Large configurations, such as one with 300 MDT default tunnels.

  The following is an example of an MVPN configuration where this problem can be seen:

  1. OSPF routing protocol is enabled on all the networks in the topology.

2. Each PE router has 100 MVRFs defined (between vpn_0 to vpn_99).
3. MDT default is configured on all the mVRFs on the PE routers.
4. PE routers have an iBGP session, ONLY with the RR (route-reflector).
5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes.
6. OSPF session also exists between Routem and PE1, with Routem sending 100 OSPF routes.

In effect, the following states are present in the network:

On PE and RR routers:

1. IGP states = 100 OSPF routes.
2. BGP states = 200,010 VPNv4 routes.

On PE routers ONLY:

1. VRF sessions = 100 VRFs (vpn0 to vpn_99).
2. MDT sessions = 100 SSM sessions.

Workaround: There is no workaround.

- CSCtb32892

  Symptoms: Tracebacks such as:

  ```
  %MFIB-3-DECAP_OCE_CREATION_FAILED: Decap OCE creation failed
  ```

  may be be seen on a router console when loading an image or during an RP SSO.

  Conditions: The symptom is observed upon reloading a Provider Edge (PE) router with an mVPN configuration or during a simple SSO. It is observed on the standby RP.

  Workaround: There is no workaround.

- CSCtb92791

  Symptoms: The command **ip ospf message-digest-key** in interface mode may have an invalid key.

  Conditions: The symptom is observed when “parser config cache interface” is configured.

  Workaround: Use the command **no parser config cache interface**.

- CSCtc59535

  Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

  Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

  Workaround: Unplug and plug back the cable.

- CSCtc68910

  Symptoms: Unnecessary retransmission and spurious TCP is reset.

  Conditions: The symptom is observed when using NAT and a large (already fragmented) “updatecabilitiesversion2” traverses the router.

  Workaround: There is no workaround.

  Further Problem Description: This problem seems to be correlated to:

  - IP phone presents an updatecabilitiesversion2 large packet (i.e.: 2012 bytes) fragmented (i.e.: in 4 pieces).

- CSCtd27247

  Symptoms: The router crashes when doing concurrent VRF add and deletion configurations.

  Conditions: The symptom is observed when a multiple configuration terminal is doing concurrent VRF add and deletion configurations.

  Workaround: Do not do concurrent VRF addition and deletion.

- CSCtd34887

  Symptoms: Performing a shut and no-shut on a subinterface with igmp-join causes SSM VRF mroute to disappear.

  Conditions: SSM VRF mroute present in the table:

```
ce#show ip mroute vrf management
(Src 1  IP, Grp IP), 00:10:48/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
(Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
```

  configuration of the interface:

```
int FastEthernet4.3
 encapsulation dot1Q 33
 ip vrf forwarding management
 ip address <IP addr>  255.255.255.252
 ip pim sparse-mode
 ip igmp join-group <group addr> source 10.32.178.56
 ip igmp join-group <group addr> source 10.32.178.23
```

  Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, the **no ip igmp-join** and **ip igmp join** commands are entered on the interface.

- CSCtd47338

  Symptoms: The following error message is constantly displayed:

```
crypto_engine_ps_vec(): no subblock attached
```

  Conditions: This issue is observed on a Cisco 7200 series router with VSA cards, that is running Cisco IOS Release 12.4(15)T (other releases may be affected as well) and with DLSw configuration.

  Workaround: Configure the command **dlsw udp-disable**.

- CSCtd90367

  Symptoms: Router crashes every 2-3 days with URLF feature. The error message shows memory leak issues.

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(24)T2, with URLF features on the device.

  Workaround: There is no workaround.

- CSCtd92028

  Symptoms: The router reloads.

  Conditions: The symptom is observed when a VRF is unconfigured while there are one or more WCCP service groups configured with that VRF.

Workaround: Unconfigure the relevant WCCP service groups prior to unconfiguring the VRF.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCtd97164

  Symptoms: LLQ packet drops on an ATM interface.

  Conditions: The symptom is observed when having QoS under an ATM interface. Packet drops are seen under a class with “priority”, even though they have not reached the value configured. It does not matter if it is percent or absolute value.

  Workaround: There is no workaround.

- CSCte02973

  Symptoms: Routing protocols like EIGRP may be dropped in the global table.

  Conditions: The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

  Workaround: Enable “ip multicast routing” and create a loopback interface with “ip pim sparse-mode” enabled.

  Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

  However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.

- CSCte10790

  Symptoms: A Cisco Catalyst 6500 series switch may unexpectedly reload due to bus error on the switching processor when making access list entry config changes or when removing an entire access-list.

  Conditions: This bug fixes two related crashes. One in which the crash occurs when making ace configuration changes and another when removing an entire ACL.

  Details on the conditions to trigger the crash when making the ace configuration changes:

  This can be reproduced in all the branches and the basic criteria reproducing this is we should have ACE is greater than 13, and we should have the extended ACE that has destination IPADDR.

  The issue is seen when we have more that three ACE which have the same source and destination address and mask and we delete the ACE in sequence like:

  ```
  no 110
  no 120
  no 130
  ```

  Then try to add ACE which has the same source address and mask but no destination. The infinite loop will result in crash.

  ```
  120 ACE
  130 ACE
  CRASH will happen
  ```

  Follow the same order:

  ```
  ip access-list extended vlan959-out
  ```

```
permit ip 128.227.128.52 0.0.0.3 any
remark - Standard out ACL -
permit tcp any any established
deny tcp any any eq 707
deny tcp any eq 707 any
deny tcp any any eq 4444
deny tcp any eq 4444 any
deny udp any any eq 31337
deny tcp any any eq 12345
deny tcp any any eq 12346
deny tcp any any eq 20034
deny tcp any any eq 7597
deny ip host 0.0.0.0 any
remark - allow cns & UFAD networks
permit ip 128.227.212.0 0.0.0.255 any
permit ip 10.227.212.0 0.0.0.255 any
permit ip 10.228.212.0 0.0.0.255 any
permit ip 10.249.10.0 0.0.0.255 any
permit ip 128.227.74.0 0.0.0.255 any
permit ip 128.227.156.0 0.0.0.255 any
permit ip 128.227.0.240 0.0.0.15 any
permit ip 10.5.187.240 0.0.0.15 any
permit ip 10.241.28.240 0.0.0.15 any
permit ip 128.227.128.112 0.0.0.3 any
permit udp 128.227.128.0 0.0.0.255 eq ntp 10.241.33.0 0.0.0.255
permit udp 128.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
permit tcp 128.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
permit tcp 128.227.156.0 0.0.0.255 host 10.241.33.11 eq www
permit tcp 128.227.128.0 0.0.0.255 host 10.241.33.29 eq cmd
```

Then follow the order:

```
no 110
no 120
no 130
120 permit udp 128.227.128.0 0.0.0.255 eq domain any
130 permit tcp 128.227.128.0 0.0.0.255 eq domain any
```

Workaround: The ACE configuration change crash can be worked around by deleting the entire ACL and then add the resequenced ACE.

The crash when removing the access-list itself has no workaround.

- CSCte14955

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router may experience an unexpected reload.

  Conditions: The symptom may occur when multiple tunnel interfaces are configured with **mpls bgp forwarding**, if the tunnel interfaces are flapping.

  Workaround: Configure the eBGP sessions on interfaces other than tunnel interfaces.

- CSCte17284

  Symptoms: A router may unexpectedly reload due to software forced crash because of chunk memory corruption.

  Conditions: The crash appears to happen when using the clientless web proxy method. The crash is triggered by accessing a webpage through the SSL VPN with a URL longer than 1009 characters long.

  Workaround: If possible, redesign the website to use URLs of 1009 characters or shorter.

- CSCte38855

  Symptoms: Chunk leak is seen after exec-timeout expires.

  Conditions: The symptom is observed after the **interface range** command is configured and when the console timeout expires.

  Workaround: There is no workaround.

- CSCte39643

  Symptoms: If PfR receives an EIGRP route change, the router may unexpectedly reload.

  Conditions: The symptom is observed with PfR and EIGRP configurations. It is observed some time after PfR receives an EIGRP route change, but before the previous EIGRP route is removed in the routing table, when PfR tries to recycle a previous EIGRP route.

  Workaround: There is no workaround.

- CSCte41410

  Symptoms: TCP connections may get stuck when using SSLVPN with **webvpn cef** configured. These connections will be stuck in TIMEWAIT state and will not timeout after the usual minute or so and will stay around forever.

  Conditions: This symptom occurs when using SSLVPN with **webvpn cef** configured.

  Workaround: Issue the **no webvpn cef** command.

- CSCte48009

  Symptoms: The NAS-Port and NAS-Port-ID AAA Attributes are not sent in radius messages.

  Conditions: The symptom is observed if the VCI value configured on the interface is larger than 32767.

  Workaround: Use VCI values less than 32767.

- CSCte49283

  Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

  Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

  Workaround: There is no workaround.

- CSCte54807

  Symptoms: Configuring PVC with Cisco IOS Release 15.0(1)M1 brings up a virtual-access interface, right after sending the ConfReq, even if there is no reply.

  Conditions: The symptom is observed when using a PPPoA setup on Cisco IOS Release 15.0(1)M1. It is seen only if some unused ATM PVCs are present at one end with the PPP configurations applied on them.

  Workaround: Use Cisco IOS Release 12.4(24)T2.

- CSCte62453

  Symptoms: Performing a shut and no-shut on a subinterface with igmp-join causes SSM VRF mroute to disappear.

  Conditions: This symptom is observed when SSM VRF mroute is present in the table:

```
ce#show ip mroute vrf management (Src 1 IP, Grp IP), 00:10:48/stopped, flags: sPLTXI
Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
Outgoing interface list: Null
(Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
Outgoing interface list: Null
```

  In addition, the interface is configured as follows:

```
int FastEthernet4.3
encapsulation dot1Q 33
ip vrf forwarding management
ip address <IP addr> 255.255.255.252
ip pim sparse-mode
ip igmp join-group <group addr> source 10.32.178.56
ip igmp join-group <group addr> source 10.32.178.23
```

  Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, the **no ip igmp-join** and **ip igmp join** commands are entered on the interface.

- CSCte63156

  Symptoms: Router hangs and crashes when a DHCP pool configured with “origin aaa subnet” is removed.

  Conditions: The symptom is observed when pool is configured with “origin aaa subnet ...” and without unconfiguring this command, the pool is deleted with the **no ip dhcp pool** command. Also missing is “aaa accounting” with “default method-list” from global configuration.

  Workaround: Globally configure “aaa accounting” with “default method-list” (“aaa accounting network default”).

- CSCte76513

  Symptoms: If ZBF and WAAS are configured on a router, you may see drop logs similar to the following:

```
%FW-6-DROP_PKT: Dropping tcp session x.x.x.x y.y.y.y due to No zone-pair between zones
with ip ident 0

%FW-6-DROP_PKT: Dropping http session x.x.x.x y.y.y.y on zone-pair admin-to-wan class
admin due to Invalid Flags with ip ident 0
```

  Conditions: The symptom is observed if ZBF and WAAS are configured on a router.

  Workaround: There is no workaround.

- CSCte78165

  Symptoms: Device may reload when the **show ip protocol** command is issued.

  Conditions: The symptom is observed when routing protocol is configured and the ISIS routes are being redistributed.

  Workaround: Do not use the **show ip protocol** command.

- CSCte82917

  Symptoms: On a Cisco 7600 series RSP720, the **show proc cpu sort** command displays a CPU utilization of 0, but the per-process CPU utilization is 100% for some processes; no packet loss occurs, however.

  Conditions: This symptom is observed under the following conditions:

  - The router is decently loaded.
  - HSRP is enabled in an HA environment.
  - A large number of HSRP sessions are established.

  Workaround: Reduce the number of HSRP sessions to only a few. The router does not see any performance or functional impact. This is an issue only with internal CPU accounting.

- CSCte83779

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router may crash.

  Conditions: The symptom is observed when DMVPN is configured with GETVPN. It is only seen when running a specific script for ASRs.

  Workaround: There is no workaround.

- CSCte89436

  Symptoms: Router crashes.

  Conditions: The symptom is observed when encapsulation is changed from from “frame-relay” to “hdlc”.

  Workaround: There is no workaround.

- CSCte96453

  Symptoms: Switch intermittently crashes when configuring energywise features.

  Conditions: The symptom is observed when the port is configured with “energywise level 10” to bring up a previously down port.

  Workaround: There is no workaround.

- CSCte98082

  Symptoms: PPPoE session is not coming up on some clients due to a malformed PADO. PPPoE relay sessions are failing to come up on an LAC.

  Conditions: The symptom is observed with a few clients which are unable to process malformed PADO and also when “pppoe relay service” is configured on the LAC.

  Workaround: There is no workaround.

- CSCtf00427

  Symptoms: A router may experience a severe memory leak issue when the following command is configured:

  privilege exec level *level* **show ip ospf neighbor**

  Conditions: The symptom is observed when running Cisco IOS Release 12.2(33)XNE or 12.2(33)XNE1. The issue is not platform dependent.

  Workaround: Reload the router.

- CSCtf04954

  Symptoms: When the **cns config notify** command exists, some CLIs might misbehave or cause unexpected crashes during the configuration change.

Conditions: The symptom is observed with the **cns config notify** command.

Workaround: Remove all **cns config notify** CLIs from the configuration.

- CSCtf06436

  Symptoms: Continuous high CPU usage.

  Conditions: The symptom occurs after the formation of a recursion loop in the FIB, when the prefixes in the loop are labeled.

  Workaround: There is no workaround.

- CSCtf08864

  Symptoms: Incoming ISDN T1/E1 PRI voice calls may disconnect or fail to complete properly. When an incoming call is made, the following symptoms may be noticed in the output of **debug isdn q921** and/or **debug isdn q931**:

  1. Q.921 debugs may report "**ERROR**: L2_AdvanceVA: TX_ack_queue empty", after which the B-channel used for the call attempt locks up. The ISDN provider needs to reset the B-channel in order to return it to service.
  2. Q.931 debugs may show that a voice call disconnected prematurely.
  3. Q.921 debugs may intermittently duplicate messages such as Receiver Ready (RR) Polling exchanges, Info frames, or SABME frames.

  Conditions: The symptom is observed on a Cisco ISR G2 2900/3900 Voice Gateway which has been installed with a VWIC2 T1/E1 MultiFlex Trunk card, configured for ISDN PRI voice services, and running a Cisco IOS 15.0 or 15.1T release. The following conditions are observed:

  1. The VWIC2 generation of T1/E1 MultiFlex Trunk cards must be used.
  2. This is a problem affecting PRI voice installs. Data PRI installs are not affected.
  3. This is an ISR G2 2900/3900 platform-specific issue.

  Not all PRI voice installs will be affected by this problem. It depends on how HDLC is configured on the PRI lines by the provider. To be specific, if the provider sends marks (all-ones) instead of HDLC flags during idle times, the call completion problem may manifest itself. Most provider installations are not configured this way and the provider may be able to switch the method of indicating an idle.

  Workaround 1: Ask the service provider to send flags between frames instead of idle marks. Idle marks (11111111) may be sent to fill the gap between useful frames. Alternatively, a series of flags (01111110) may be transmitted to fill gaps between frames instead of transmitting idle marks. Continuous transmission of signals is required to keep both the transmitting and receiving nodes synchronized.

  Workaround 2: If Workaround 1 is not possible, a Cisco IOS image with a candidate fix is available. The candidate fix has a high confidence level of resolving the PRI voice call issues described above, and has proven to be successful in several field deployments complaining of similar call problems. Please contact the Cisco Technical Assistance Center (TAC) for details on obtaining the candidate fix.

- CSCtf18077

  Symptoms: A CME router may unexpectedly reload due to a bus error when a Cisco Unified Contact Center Express (UCCX) unregisters from the CME.

  Conditions: The symptom is observed when the Cisco UCCX unregisters from the CME.

  Workaround: There is no workaround.

- CSCtf18524

  Symptoms: Throughput performance for HTTP traffic is impacted.

  Conditions: The symptom is observed when the SSLVPN feature is configured on the router and crypto engine is configured to accelerate the SSLVPN feature.

  Workaround: There is no workaround.

- CSCtf19461

  Symptoms: IP address is not leased out to the client from server.

  Conditions: The symptom is observed when configuring the VPN sub-option at the interface level on the relay.

  Workaround: There is no workaround.

- CSCtf25293

  Symptoms: SSH connection to a SSH server aborts abruptly after making the connection, while using public key-based authentication.

  Conditions: Authentication method used must be public key.

  Workaround: Use kbd-interactive or password-based authentication.

- CSCtf27303

  Symptoms: On a Cisco router, a BGP session for a 6PE (peer-enabled in AF IPv6 and end-label configured) with a third-party router, which does not advertise capability IPv6 unicast (not AFI 2 SAFI 1, only AFI 2 SAFI 4) may be torn down right after it establishes, as the Cisco router sends out an update in the non-negotiated AF IPv6 unicast (AFI/SAFI 2/1).

  Conditions: The symptom is observed under the following conditions:

  - Cisco side: session enabled for IPv6 + send-label. Cisco router is running Cisco IOS Release 12.2(33)XNE1 and Release 12.2(33)SRE.
  - Third-party: only capability IPv6 labeled unicast advertised.

  Workaround: There is no workaround.

- CSCtf27324

  Symptoms: A ping from a CPE (which is doing PPP to the IP address of the LNS router that terminates that PPP call) fails. PPP has been opened and IPCP has negotiated an IP address. Ping from the LNS back to the CPE works fine. Between the LAC and the LNS there is a PPP multilink bundle.

  Conditions: The symptom is observed only when there is a plain PPP call from a client (ISDN modem or dial up modem which is doing PPP). In addition, the physical connectivity between the LAC and the LNS is PPP multilink.

  Workaround: Disable CEF on the physical interface between the LAC and the LNS. If the CPE is doing PPP multilink, the ping works fine.

  Further Problem Description: The issue seems to be specific with the forwarding of the packets through the PPP multilink bundle that exists between the LAC and the LNS.

- CSCtf29685

  Symptoms: PPPoE server router crashes upon sending an accounting stop request.

  Conditions: The symptom is observed with a PPPoE setup for both PTA and forwarded case. This is seen only if template authorization is enabled (i.e.: “aaa authorization template” is configured) and some template attributes are configured in the user-profile on the radius server.

Workaround: There is no workaround.

- CSCtf31067

  Symptoms: There is no implementation for retransmitting MS-CHAP v2 challenge for PPP negotiation.

  Conditions: The symptom is observed with a MS-CHAP v2 challenge.

  Workaround: There is no workaround.

- CSCtf36117

  Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

  Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

  Workaround: There is no workaround.

- CSCtf39455

  Symptoms: Router can hang when xconnect configuration is modified on a VLAN subinterface while data packets are being switched. The following error traceback is printed:

  ```
  %SYS-2-NOTQ: unqueue didn't find 0 in queue
  ```

  Conditions: The symptom is observed when the VLAN subinterface is still seeing data traffic and the main interface is not shut down, and when the xconnect configuration on the VLAN subinterface is being modified.

  Workaround: Shut down the main ethernet interface when doing xconnect configuration changes on the subinterface.

- CSCtf40425

  Symptoms: When executing the **service-module** *interface* **install** command on an SRE module on a Cisco Integrated Services Router (ISR) G2, the router may unexpectedly reload due to a bus error.

  Conditions: The symptom is observed only when executing the install on an SRE module.

  Workaround: There is no workaround.

- CSCtf40731

  Symptoms: A routing loop is unexpectedly formed when PIRO and an OER-generated static route works together.

  Conditions: The symptom is observed under the following conditions:

  1. PIRO generates a more specific prefix for the static route it has created.
  2. OER-generated static route is redistributed into other IGP protocol in order to get traffic.

  Workaround: There is no workaround.

- CSCtf47335

  Symptoms: Wrong typedef version is returned.

  Conditions: The symptom is observed on getTypedefs CT, the typedefVersion returned is “2008-08-01”. This is the wrong version with some undefined entries. Due to this, the signature parsing is failing in CCP.

  Workaround: There is no workaround.

- CSCtf47396

  Symptoms: A Cisco router may crash when a service-policy configured with bandwidth is removed from an interface.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCtf50075

  Symptoms: A traffic blackhole can occur.

  Conditions: The symptom is observed following shut/unshut/shut of the redundant forwarding interface.

  Workaround: There is no workaround.

- CSCtf51690

  Symptoms: Router crashes when a packet with out-of-bound featureIndex values is sent to the CME.

  Conditions: The symptom is observed when malformed packets are sent to the CME with out-of-bound featureIndex values in fStationFeatureStatReqMessage.

  Workaround: There is no workaround.

- CSCtf52106

  Symptoms: There is a failure of EEM TCL scripts when using the “exit_comb” keyword for the Interface Event Detector.

  Conditions: The symptom is observed when using the “exit_comb” keyword in an EEM TCL script.

  Workaround: There is no workaround.

- CSCtf57641

  Symptoms: A router crashes after performing a DNS lookup.

  Conditions: The symptom is observed when a command is used which sends out a DNS query such as **ping www.cisco.com** and the DNS server response contains a specially crafted packet.

  Workaround: Configure “no ip domain-lookup”.

- CSCtf62621

  Symptoms: Unable to push the firewall down to the VDSL chipset on a Cisco 887V modem.

  Conditions: The symptom is observed on a Cisco 887V router with no startup configuration in NVRAM.

  Workaround: Perform a **write memory** and reload the router.

- CSCtf66271

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router that was running the asr1000rp1-adventerprisek9.02.04.02.122-33.XND2.bin image and then upgrades to the asr1000rp1-adventerprisek9.02.06.00.122-33.XNF.bin image displays the complete certificate chain as follows:

  ```
  crypto pki certificate chain JUTnetRoot-Pilot certificate ca
  3C5A00179190F2DF23325330195B9B67 308203AE 30820296 A0030201 0202103C 5A001791 90F2DF23
  32533019 5B9B6730 0D06092A 864886F7 0D010105 05003071 310B3009 06035504 06130255
  53311930 17060355 040A1410 41542654 20436F72 706F7261 74696F6E 311F301D 06035504
  0B131646 6F722054 65737420 50757270 6F736573 204F6E6C <truncated>
  ```

  whereas before the upgrade it displayed:

```
crypto pki certificate chain JUTnetRoot-Pilot certificate ca
3C5A00179190F2DF23325330195B9B67 nvram:ATTCorporati#9B67CA.cer
```

Conditions: The symptom is observed with a Cisco ASR 1006 router that is running the asr1000rp1-adventerprisek9.02.06.00.122-33.XNF.bin image.

Workaround: There is no workaround.

- CSCtf67170

  Symptoms: There is a crash due to the following error:

  ```
  %ALIGN-1-FATAL: Illegal access
  ```

  Conditions: The symptom is observed when “call monitor” is configured.

  Workaround: Remove call monitor, if interfacing with UCCX is not needed.

- CSCtf70959

  Symptoms: EzVPN client is trying to negotiate the connection with a NULL address when the outside interface is a profile-based dialer interface.

  Conditions: This situation is a corner condition. The IP address on the dialer interface will be installed as soon as the dialer negotiation completes and the dialer interface comes up. But in this case, even though the IP address is not installed the dialer interface, the API is returning TRUE and proceeds further with the EzVPN connection.

  Workaround: Use a non profile-based dialer interface.

- CSCtf71010

  Symptoms: Traffic does not flow through the hub.

  Conditions: The symptom is observed when a Cisco 3900 series router is configured for VRF-aware tunnel protection for IKEv2 sessions.

  Workaround: There is no workaround.

- CSCtf71990

  Symptoms: An alert message is not sent if “source-ip-address” is configured in the call-home configuration. The following message is shown:

  ```
  %CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP servers (ERR
  7, error in connecting to SMTP server)
  ```

  Conditions: The symptom is observed when “source-ip-address” is configured.

  Workaround: Remove “source-ip-address”.

- CSCtf75053

  Symptoms: DHCP Relay will send a malformed DHCP-NAK packet. The malformed packet will be missing the END option (255) and the packet’s length will be truncated to 300. In effect, all the options after 300 bytes, if any, will be missing.

  Conditions: When a Cisco 10000 series router is configured as a relay and a DHCP request is sent from the CPE, the router will send a DHCP-NAK when client moves into a new subnet.

  Workaround: There is no workaround.

- CSCtf78196

  Symptoms: Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

Conditions: The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface. (It is seen on many images)

Workaround: Statically configure “ipv6 mtu <mtu>” on tunnel interfaces.

- CSCtf80105

  Symptoms: When basic SIP-SIP calls are placed using automation scripts, calls start failing due to UDP socket connection error

  Conditions: The symptom is observed when the router is configured with a dial peer and with SNMP. A dial peer is most likely required to reproduce the issue, but it is possible that a different UDP protocol other than SNMP could also cause the symptom. Once a call failure occurs, all the calls placed later will fail with a UDP socket connection error.

  Workaround: Use the following steps:

  1. Under sip-ua, configure “connection-reuse” (which is a hidden command).
  2. Configure the use of TCP.

- CSCtf81271

  Symptoms: When “station-id name” or “station-id number” is configured on a voice port, “caller-id enable” will also be configured on that voice port.

  Conditions: The symptom is observed after upgrade to Cisco IOS Release 12.4(22)T or Release 12.4(24)T where the **caller-id enable** command gets auto-configured on the voice-port.

  Workaround: Manually remove the **caller-id enable** command after a router reboot.

- CSCtf82883

  Symptoms: When clearing a VRF route, there is a traffic drop on other VRF routes.

  Conditions: The symptom is observed with an L3 VPN configuration.

  Workaround: There is no workaround.

  Further Problem Description: Some LTE broker distribution is leaked to other VRFs.

- CSCtf83092

  Symptoms: Standby resets continuously while ISSU upgrade from a non-componenterized IOS image to a componenterized IOS image.

  Conditions: The issue is seen with an MPLS VC configuration.

  Workaround: There is no workaround.

- CSCtf83101

  Symptoms: Packets are not correctly classified by QoS class-map in CEF switching. Priority packets are dropped even if they are classified into LLQ. This is shown by the **show policy-map interface** command.

  Conditions: The symptom is observed under the following conditions:

  - A BRI interface.
  - LLQ is configured on egress port by policy-map.
  - The following devices/platforms are used: HWIC-4B-S/T or HWIC-1B-U, Cisco 181x, Cisco 180x, Cisco 800.

  Workaround: Disable CEF.

  Alternate Workaround: Use the other HWIC or WIC.

- CSCtf85219

  Symptoms: The following symptoms are seen:

  - No dial tone when going off hook, so other phone numbers cannot be dialed.
  - The hung port can receive incoming calls, however the originating phone hears ring back. The terminating phones rings but when the call connects there is one-way audio.

  Conditions: The symptom is observed with STCAPP-controlled FXS ports.

  Workaround: Perform a shut/no shut on the voice port. If this does not work, perform a reload.

- CSCtf86556

  Symptoms: The middle router crashes when it receives a PathTear message.

  Conditions: The symptom is observed when the middle router (that does not have SREFRESH configured) receives a PathTear message, when the session debug is on.

  Workaround: Disable the session debugs.

  Alternate workaround: Configure refresh reduction on the UUT.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

  Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

  Workaround: There is no workaround.

- CSCtf96538

  Symptoms: ATM interface does not pass/receive traffic. The configuration on the ATM interface shows “atm scrambling cell-payload” configured, but the **show controller ATM** output shows “DS3 Scrambling OFF”.

  Conditions: The symptom is observed on a Cisco 3925 router, with an NM-1A-T3/E3 and running a Cisco IOS 15.0 release.

  Workaround: Disable scrambling on the network.

- CSCtf91428

  Symptoms: Router crashes in IP Input.

  Conditions: NAT needs to be configured.

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

  The public interface was an ATM [DSL].

  Workaround: Disable

  ip nat service for h232 - rass

  Disable CEF globally.

- CSCtf97322

  Symptoms: Shaping is not working correctly. An additional symptom on a Cisco 2900 series router is the possibility of alignment errors and, in rare situations, a software-forced crash.

  Conditions: The symptom is observed on Cisco 2900 and 3900 series routers when using one of the following serial modules: HWIC-1T, HWIC-2T and HWIC-1DSU-T1.

  Workaround: There is no workaround.

- CSCtg02719

  Symptoms: Informers reload.

  Conditions: The symptom is observed when enabling the **voice dsp crash-dump** or **debug vpm dsp** commands. These two commands may cause Informers to reload.

  Workaround: Do not enable the **voice dsp crash-dump** or **debug vpm dsp** commands on Informers.

- CSCtg06863

  Symptoms: The **show processes cpu sorted** command will incorrectly show processes with CPU utilization of 100%. Also, CPU utilization will vary randomly.

  Conditions: The symptom is always observed when traffic is flowing through the router and may or may not be seen without traffic flowing.

  Workaround: There is no workaround.

- CSCtg07557

  Symptoms: A reload of a Cisco 1941W-A/K9 causes the embedded AP 801 to go to ROMMON. The AP BOOT parameter is no longer set and the startup configuration is also erased.

  Conditions: The symptom is observed when a reload is issued on the router and you reload the AP at the same time when prompted.

  Workaround: When reloading router using CLI, answer "no" when prompted to reload the embedded AP. The embedded AP can be reloaded with the **service-module wlan-ap 0 reload** command from router console or the **reload** command from embedded AP console accessed via **service-module wlan-ap 0 session.**

- CSCtg08496

  Symptoms: After merge, keyserver deletes all GMs so the rekey fails to be sent (DB is empty) and all the GMs need to re-register.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtg09379

  Symptoms: After upgrading to an IOS build with EnergyWise specification: (rel2_5)1.0.32, the switch crashes several hours later.

  Conditions: The symptom is observed when activity check is on and recurrence is changed from 0 to a higher value.

  Workaround: There is no workaround.

- CSCtg11186

  Symptoms: A router may face a watchdog crash or hang while removing a port-channel.

  Conditions: The symptom is observed with a Cisco 3900/2951 router when removing a port-channel interface. It is seen when PPPoE is enabled on the GE interface.

  Workaround: There is no workaround.

- CSCtg13758

  Symptoms: Router can crash due to corrupted magic value in freed chunk.

  Conditions: The symptom is observed on a Cisco 881 router that is running Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCtg17600

  Symptoms: The configured “egress-method negotiated-return” does not work.

  Conditions: The symptom is observed with VRF-aware WCCP and with Cisco IOS Release 15.1(1)T. The WCCP return traffic arrives on a sub-interface.

  Workaround 1: Do not configure “egress-method negotiated-return”.

  Workaround 2: If “egress-method negotiated-return” is configured ensure that the interface on which return traffic arrives is not configured with sub-interfaces.

  Workaround 3: Change the Cisco IOS Release from 15.1(1)T to 15.0M.

- CSCtg20254

  Symptoms: Router crashes.

  Conditions: The symptom is observed when “debug glbp event” is turned on.

  Workaround: There is no workaround.

- CSCtg23251

  Symptoms: Analog phones lock up and there is no dial tone.

  Conditions: The symptom is observed when the CME is in fallback as SRST and a directed call park is attempted on analog phones. The user cannot pick up a call from a park slot by direct dialing the slot. In the event that the user is able to retrieve the call, when the call is hung up the channel is not released. No dial tone is heard when the handset is picked up again.

  Workaround: Reset the ports.

- CSCtg28806

  Symptoms: Router crashes at PKI manual enroll.

  Conditions: The symptom is observed on a Cisco 2921 router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg36728

  Symptoms: Router crash or spurious memory access can be seen.

  Conditions: The symptom is observed if non-default locale is enabled and a UCME receives a make call request from UCXSI with the “prompt” option.

  Workaround: There is no workaround.

- CSCtg38344

  Symptoms: Upon a reload, a router may lose most of its configuration after the pubkey-chain user/server sub-mode is gone. The following error is reported during the reboot:

  ```
  Installed image archive Cisco 1841 (revision 5.0) with 237568K/24576K bytes of memory.
  Processor board ID 6 FastEthernet interfaces 2 Virtual Private Network (VPN) Modules 2
  802.11 Radios DRAM configuration is 64 bits wide with parity disabled. 191K bytes of
  NVRAM. 62720K bytes of ATA CompactFlash (Read/Write)
  bridge irb ^ % Invalid input detected at ‘^’ marker.
  interface FastEthernet0/0 ^ % Invalid input detected at ‘^’ marker.
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 15.0(1)M2 with “ip ssh pubkey-chain” configured.

  Workaround: Remove the SSH keys before upgrading to Cisco IOS Release 15.0(1)M2 or Release 15.1(1)T.

- CSCtg40901

  Symptoms: Crash seen while authenticating with TACACS.

  Conditions: The symptom is observed if the TACACS server does not respond.

  Workaround: Use multiple connections.

  Alternate Workaround: Configure a dummy TACACS server.

- CSCtg41232

  Symptoms: Traffic, set to be exempted from inspection via an extended ACL, is still inspected even though the ACL registers counts for that traffic.

  Conditions: The symptom is observed on any Cisco access router that is running Cisco IOS 15.x code.

  Workaround: There is no workaround.

- CSCtg41733

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

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

  Workaround: Disable SIP if it is not needed.

- CSCtg45099

  Symptoms: Router crashes.

  Conditions: The symptom is observed when the **show cca** command is issued.

  Workaround: There is no workaround.

- CSCtg54272

  Symptoms: Router may crash when upgrading modem firmware.

  Conditions: The symptom is observed with a Cisco 880 router that is running Cisco IOS interim Release 15.1(0.26)T.

  Workaround: There is no workaround.

- CSCtg56013

  Symptoms: Router crashes when initiating ping through the modem after router bootup.

  Conditions: The symptom is observed when the modem fails to enumerate at bootup.

  Workaround: There is no workaround.

- CSCtg57623

  Symptoms: Music on hold does not work with iLBC codec when an IOS transcoder is used.

  Conditions: The symptom is observed when the phone is configured to use iLBC codec and a transcoder is invoked to transcode MOH G.711 audio stream to iLBC codec. The phone rejects the RTP stream due to incorrect payload-type (it sends payload type 118 instead of the correct 116 for iLBC).

  Workaround: There is no workaround if iLBC codec is needed, but using a different codec at the remote phone should work.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

Workaround: There is no workaround.

- CSCtg63942

  Symptoms: The output of **show proc cpu sorted** is not correct. The total CPU displayed is always 0, even though the interrupt level CPU displayed is a non zero value. Total CPU should be the sum of the interrupt and process level CPU. Consequently, the values displayed by **show proc cpu history** are also incorrect.

  Conditions: The symptom is observed when using the **show process cpu sorted** command.

  Workaround: There is no workaround.

- CSCtg65763

  Symptoms: The command **clear crypto gdoi** on the keyserver does not clear the keyserver policies.

  Conditions: The symptom is observed once the keyserver policies have been created.

  Workaround: There is no workaround.

- CSCtg73691

  Symptoms: You cannot configure “route-target import” or other BGP extended community values with values greater than 65535 to the right of the “:” even though you are using a value less than 65536 to the left of the “:”.

  Conditions: This is seen when you issue a route-target import command with a value less than 65536 to the left of the “:” (and no “.” to the left of the “:”) and a value greater than 65535 to the right of the “:”.

  Workaround: There is no workaround.

  Further Problem Description: This problem was introduced by CSCtf13343.

  The following formats are supposed to be accepted:

  1. <IPv4 address>:<16-bit number>.
  2. <2-byte ASN>:<32-bit number>.
  3. <4-byte ASN in asplain format>:<16-bit number>.
  4. <4-byte ASN in asdot format>:16-bit number.

- CSCtg79105

  Symptoms: A UC560 unexpectedly reboots.

  Conditions: The symptom is observed when the **show memory 0** command is executed.

  Workaround: There is no workaround.

- CSCtg86714

  Symptoms: The **show cellular 0** command might not show any output.

  Conditions: The symptom is observed with the **show cellular 0** command.

  Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the “MODEM UP” line, you get “LINK UP” and still retain the **show cellular stats**.

- CSCtg88766

  Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

  Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

Workaround: There is no workaround.

- CSCtg93243

  Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

  Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used packets get forwarded after decryption as expected.)

  Workaround: There is no workaround.

- CSCtg99114

  Symptoms: The following error message with traceback is observed:

  ```
  %IPC-5-REGPORTFAIL: Registering Control Port
  ```

  Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.

  Workaround: Drop IPC traffic using control-plane policing:

  ```
  class-map match-all ipc
  match access-group name ipc
  policy-map drop-ipc
  class ipc
  drop
  ip access-list extended ipc
  permit udp any any eq 1975
  control-plane
  service-policy input drop-ipc
  ```

- CSCth02789

  Symptoms: System can crash when attempting to schedule an IPv6 icmp-echo operation.

  Conditions: The symptom is observed with IPv6 and icmp-echo.

  Workaround: There is no workaround.

- CSCth15518

  Symptoms: Ping through ISDN BRI interface fails.

  Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.

  Workaround: There is no workaround.

- CSCth35620

  Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

  Conditions: The symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

  Workaround: There is no workaround.

- CSCth39774

  Symptoms: UUT hangs when an eTCDF file is loaded on the router in the latest t_base_1 code base.

  Conditions: The symptom is observed when an eTCDF file is loaded on the router, the UUT seems to hang. However, the UUT is actually waiting for user input, and if you enter “#” on the CLI, it will print some error messages about invalid commands and return to CLI.

Workaround: Do not use the eTCDF file to configure the encrypted filter, rather directly enter the commands on the CLI of the router.

- CSCth47765

  Symptoms: Once a router boots up, FXS/FXO voice-port in slot2 stays in "S_OPEN_PEND" state. The DSP from the MB that provides resources to the EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards in slot 2 goes into "FW_DNLD_FINISHED" state which causes the voice ports on EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards to go into "S_OPEN_PEND state".

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(1) T0.9 with 26.8.0 DSPware.

  Workaround: There is no workaround.

- CSCth51125

  Symptoms: PCEX-3G-HSPA-R6 is not recognized at bootup:

  ```
  %CISCO800-2-MODEM_NOT_RECOGNIZED: Cellular0 modem not RECOGNIZED. Carrier id not
  available or invalid! Replace it with Cisco supported modem and reload the router.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  ```

  Conditions: The symptom is observed on a Cisco 881G-K9 that is running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCth59217

  Symptoms: Firewall sessions are not seen when ZBFW and and gatekeeper are configured on the UUT.

  Conditions: The symptom is observed when ZBFW and gatekeeper are configured on the UUT.

  Workaround: There is no workaround.

- CSCth79353

  Symptoms: A Cisco 3900 series router may experience a software-forced reload when running Cisco IOS Release 15.0(1)M1.

  Conditions: The symptom is observed when the router has a QoS policy attached to one of the LAN interfaces. The QoS policy needs to match different ACLs and have shaping configured.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(1)T

All the caveats listed in this section are open in Cisco IOS Release 15.1(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsl64247

  Symptoms: Router crashes 20-30 minutes after configuring "mode route control".

  Conditions: The symptom is observed when the router is configured as OER master.

  Workaround: There is no workaround.

- CSCsm82554

  Symptoms: A router may unexpectedly reload if the device runs out of memory and a call is setup.

Conditions: The symptom is observed in rare circumstances when the device is already out of memory.

Workaround: There is no workaround.

- CSCsu24321

  Symptoms: Router crashes due to a bus error in IOS firewall.

  Conditions: This symptom occurs on a Cisco 3825 router running Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCsu64365

  Symptoms: The system may experience repeated crash due to I/O memory corruption showing error messages like:

  ```
  %SYS-6-BLKINFO: Corrupted next pointer blk
  ```

  Conditions: The corruption is caused by voice packets encapsulated by GRE/IPSEC (other encapsulations which add to the size of the packet). The router must have voice packets routed through GRE or IPSEC tunnel and if a simultaneous Fax tone is sent, the router will crash.

  Workaround: Move the GRE tunnel from the CME where ever possible.

- CSCsu66197

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

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsv81150

  Symptoms: A Cisco AS5400-XM may encounter the following error messages:

  ```
  %SYS-2-MALLOCFAI L: Memory allocation of 190 bytes
  failed from 0x6237F000, alignment 0 Pool: Processor  Free: 630453896  Cause:
  Interrupt level allocation
  Alternate Pool: None  Free: 0  Cause: Interrupt level allocation
  -Process= "<interrupt level>", ipl= 3,

  %SYS-3-INTPRINT: Illegal printing attempt from interrupt level.

  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level,

  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level,
  ```

  Conditions: The symptom is observed with a Cisco AS5400-XM that is running Cisco IOS Release 12.4(15)XY2.

  Workaround: There is no workaround.

- CSCsv86234

  Symptoms: The Cisco Gateway GPRS Support Node (GGSN) may stop forwarding packets for PDPs that are configured for the “network behind mobile” feature after a failover.

  Conditions: This issue is seen only for “network behind mobile” PDPs after a failover.

  Workaround: There is no workaround.

- CSCsv97424

  Symptoms: Router crashes due to memory corruption in the I/O pool. In all of the crashes previous block pointer is corrupted.

  Conditions: This symptom is observed in a Cisco 2811 that is running Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsy30256

  Symptoms: A Cisco 2811 router crashes due to a bus error after an ISDN call terminates. The following is seen before the crash:

```
%ALIGN-1-FATAL: Corrupted program counter
  pc=0x0 , ra=0x400ABA78 , sp=0x44647440


 TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x0
```

  Conditions: The symptom is observed when "dialer rotary-group *number*" is configured on the interface.

  Workaround: Use "dialer pool" instead of "dialer rotary".

- CSCsy85375

  Symptoms: The asynchronous interface of the V.92 modem in a Cisco 1800/890 series router reports input CRC and abort errors when connected with a PVDM2-DM modem module and using V.44 compression. This issue can cause data packet loss.

  Conditions: This issue occurs when a V.92 modem which is built in a Cisco 1800/890 series router connects to PVDM2-xxDM modems and is connected with V.44 compression. If V.44 compression is not negotiated, this issue will not occur.

  Workaround: Disable the V.44 compression by configuring the 1800/890 modem to negotiate V.42bis by using the below mentioned modemcap. Also, you need to override the system default chat-script with your own, as the system default chat-script will issue the **ATZ** command, which will do a reset of modem, thus the modemcap settings will be lost.

```
1811 V.92 modemcap:
modemcap entry V.42bis:MSC=&FN4%C0+DS=3
```

  Sample chat-script:

```
chat-script dial "" "ATDT" TIMEOUT 60 CONNECT p
```

  Sample line configuration to apply the above chat-script.

```
line 1
 script dialer dial
 modem InOut
 no exec
 transport input all
 transport output all
 stopbits 1
 speed 115200
 flowcontrol hardware
```

- CSCsz70049

  Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the telco side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.

  Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.

  Workaround: Issue the **clear interface bri** command to restore this state.

- CSCta06451

  Symptoms: Memory leak is observed in export packets when both OER and Netflow are enabled.

  Conditions: The symptom is observed only when both Netflow and OER export is enabled. OER export is enabled by default to a 3949 port.

  Workaround: There is no workaround.

- CSCta08870

  Symptoms: A memory leak can occur in the VTSP process, due to calls failing to clear completely.

  Conditions: The symptom is observed with the VTSP process.

  Workaround: There is no workaround.

- CSCta13745

  Symptoms: VM notifications sent from CUE to CME SIP trunk may have no audio.

  Conditions: The symptom is observed with a SIP trunk and VM notifications sent to PSTN over the SIP trunk.

  Workaround: There is no workaround.

- CSCta28282

  Symptoms: The Null0 route advertised via VPNv4 flaps.

  Conditions: The issue is seen on a Cisco 7200 series router with the Cisco IOS interim Release 15.0(1)M1.10 image

  Workaround: There is no workaround.

- CSCta42633

  Symptoms: Ping fails to a directly-connected router after removing “frame-relay payload-compression”.

  Conditions: The symptom is observed only if “frame-relay payload-compression” is removed on both the routers connected back-to-back.

  Workaround: Remove and re-apply the frame-relay map-class under the interface on both the routers connected back-to-back.

- CSCta55561

  Symptoms: Per-VRF dampening is not supported.

  Conditions: The symptom is observed during normal code flow.

  Workaround: There is no workaround.

- CSCta58068

  Symptoms: During BGP convergence, CPU spike may be seen on the local PE in an MVPN configuration after conditions.

Conditions: Conditions causing excessive BGP convergence and high CPU utilization (with and without traffic) in an MVPN setup can be varied as:

- Remote PE neighbor switchover
- On local PE, do a **clear ip bgp** *bgp nbr.*
- On bringup of local PE
- Large configuration such as one with 300 MDT default tunnels.

Here is an example of an MVPN configuration where this problem can be exhibited:

1. OSPF routing protocol is enabled on all the networks in the topology.
2. Each PE router has 100 MVRFs defined (between vpn_0 to vpn_99)
3. MDT default is configured on all the mVRFs on the PE routers
4. PE routers have an iBGP session, ONLY with the RR (route-reflector)
5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes
6. OSPF session also exists between Routem and PE1, with Routem sending 100 OSPF routes

In effect the following states are present in the network:

On PE and RR routers:

1. IGP states = 100 OSPF routes
2. BGP states = 200,010 VPNv4 routes

On PE routers ONLY:

1. VRF sessions = 100 VRFs (vpn0 to vpn_99)
2. MDT sessions = 100 SSM sessions

Workaround: There is no workaroun.

- CSCta78212

  Symptoms: Following an upgrade to Cisco IOS Release 12.4(15)T7 with IPS v5, there is a severe drop in throughput for customer traffic when IPS is enabled.

  Conditions: The symptom is observed with the following conditions:

  - A Cisco 1841 router that is running Cisco IOS Release 12.4(15)T7.
  - The image is c1841-advsecurityk9-mz.124-15.T7. - IPS v5.

  Workaround: Deactivate IPS from interface.

- CSCtb26941

  Symptoms: Intermittent echo on voice calls are experienced. All calls through a particular DSP channel will experience echo.

  Conditions: The symptom is observed when a DSP channel, or set of DSP channels, go into a bad state where they no longer cancel echo. The audio stream coming into the DSP will match exactly what is going out. This can be identified by the symptom that the echo-cancellation tail will vary during a call even when the tail is specified on the voice port. Values from 24ms to 112ms have been observed for a single call which this issue occurs on. The **show call active voice echo-canceller summary** command can be used to observe the echo cancellation tail, and the voice-port command **echo-cancel coverage** can be used to statically set the echo cancellation tail.

  Workaround: The DSP can be reset, or the gateway can be reloaded, and the echo canceller will begin functioning.

- CSCtb38071

  Symptoms: While testing the Large-Scale Dial-Out (LSDO) feature, the expected number of links is not seen in the bundle after starting calls in both directions for a single client. The traffic is sent for around 10 minutes. Dialer map is formed for the required address.

  Conditions: This issue is seen in a router that is loaded with Cisco IOS interim Release 12.4(24.6)PI11r.

  Workaround: There is no workaround.

- CSCtb39756

  Symptoms: New GM is not able to communicate to existing GMs.

  Conditions: The symptom is observed under the following conditions:

  1. Primary keyserver reloads.
  2. Secondary keyserver takes over role as primary and removes the old TEK and creates a new TEK2.
  3. During the period where the existing GMs have both old and new TEK keys, any new GM that registers will only get the new TEK. This new GM will not be able to communicate to the existing GMs until the old TEK expires.

  Workaround: There is no workaround.

- CSCtb42862

  Symptoms: A Cisco 3845 router crashes due to illegal memory access.

  Conditions: The symptom is observed in a scale testing environment which has eight key servers and 20 GM routers (simulating 2000 group members) and when there is unicast rekeying. The GM router crashes in steady state (no traffic). This seems to be intermittent.

  Workaround: There is no workaround.

- CSCtb47647

  Symptoms: Active RP crashes at pim_send_join_prune, when starting memory leak debugging and after executing the **show memory traceback exclusive** command.

  Conditions: To be determined.

  Workaround: There is no workaround.

- CSCtb51244

  Symptoms: Spurious memory access is seen when deleting a policy map.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 12.4(24.6)PI11u.

  Workaround: There is no workaround.

- CSCtb55576

  Symptoms: When a HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

  Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for ~160-250ms.

  Workaround: There is no workaround.

- CSCtb67800

  Symptoms: Memory leak is observed when zone-based firewall policy is configured and unconfigured.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCtb98159

  Symptoms: TCP connections made to the IP address of an interface on a Cisco 870 router are dropped when “IPSec VPN” and “protocol inspection” are configured for the same interface. TCP connections that are dropped are not made over an IPSec connection.

  Conditions: The symptom is observed under the following conditions:

  - IPSec VPN is configured for the interface.
  - Inspection is configured for the interface with the **ip inspect** command.

  TCP drops are triggered by a successful IPSec VPN session establishment and termination to the interface.

  Workaround: There is no workaround.

- CSCtb99736

  Symptoms: ISDN cause codes are not being forwarded transparently to the PBX.

  Conditions: The symptom is observed with a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T1. It is seen when the ISDN interface is configured with “isdn global-disconnect” on both sides.

  Workaround: There is no workaround.

- CSCtc06935

  Symptoms: Packet loss occurs between two Cisco Catalyst 3200 MAR routers connected over FESMIC Fast Ethernet ports via wireless radios after upgrading to Cisco IOS Release 12.4(22)T2.

  Conditions: The symptom is observed with the following conditions:

  - After a code upgrade.
  - On Cisco Catalyst 3200s connected via wireless radios.
  - It does not occur on devices directly connected via fiber.

  Workaround: Use Cisco IOS Release 12.4(1a).

- CSCtc12002

  Symptoms: An NM-1A-OC3-POM can not achieve line rate. Router performance degradation is observed.

  Conditions: The symptom is observed with an NM-1A-OC3-POM module on a Cisco 3945 router. The performance degradation issue is observed for OC3 module while trying to reach OC3 line rate with small size (64Bytes) bi-directional traffic streams. Non-drop rate and CPU utilization performance is degraded due to this issue.

  Workaround: Avoid touching line rate with small size bi-directional traffic streams (uni-directional traffic can touch line rate without any problem).

- CSCtc28073

  Symptoms: Packets are dropped when VPDN is configured as there are two IP headers added to the packet.

Conditions: The symptom is seen when VPDN is configured and CEF is enabled.

Workaround: Disable CEF.

- CSCtc33476

  Symptoms: The UUT crashes.

  Conditions: The symptom is observed when running IPv6 inspection. The issue is seen with IPv6 FTP inspections.

  Workaround: There is no workaround.

- CSCtc38922

  Symptoms: A router crashes when “ip inspect” is configured.

  Conditions: The symptom is observed when “ip inspect” is configured.

  Workaround: Disable “ip inspect”.

- CSCtc42605

  Symptoms: Memory leak can be observed when reconfiguring class-map attached to a zone-pair.

  Conditions: The symptom can be observed with a router that is running Cisco IOS Release 15.0(1)M0.1.

  Workaround: There is no workaround.

- CSCtc45177

  Symptoms: The “text_start” is not showing up in crashinfo.

  Conditions: The symptom is observed with crashinfo data.

  Workaround: There is no workaround.

- CSCtc45487

  Symptoms: On a random set of dVTI spokes, IPSec tunnels get randomly stuck. The tunnel interface on the spoke(s) goes down (administratively UP, line protocol DOWN). Traffic does not pass anymore although the crypto socket shows “UP”, crypto is up, and all looks ok, except for the line protocol is down.

  The matching virtual-access on the hub stays up. The crypto is still up and running (DPD is working and even rekey).

  Conditions: The symptom is observed with the following conditions:

  - (dVTI) terminating a large set of tunnels.
  - IPSec tunnel protection.
  - Cisco IOS Release 12.4(15)T9.

  Workaround: Do a shut/no shut of the affected tunnel interfaces.

- CSCtc59535

  Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

  Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

  Workaround: Unplug and plug back the cable.

- CSCtc68910

  Symptoms: Unnecessary retransmission and spurious TCP is reset.

Conditions: The symptom is observed when using NAT and a large (already fragmented) “updatecabilitiesversion2” traverses the router.

Workaround: There is no workaround.

Further Problem Description: This problem seems to be correlated to:

  - IP phone presents an updatecabilitiesversion2 large packet (i.e.: 2012 bytes) fragmented (i.e.: in 4 pieces).

- CSCtc71408

  Symptoms: Fax transmission fails when CUBE is in the middle.

  Conditions: The symptom is observed when either one of the dial-peers on OGW/TGW/CUBE is configured for fax protocol T38 version 0.

  Workaround: Configure version 3 on all dial-peers.

- CSCtc79092

  Symptoms: Timeout of active connections.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T1 and Release 12.4(22)T1 with ZBF enabled. The issue only occurs for TCP connections when using ZBF, and is most noticeable for RDP connections. Problem is not seen when ZBF is not configured on the interface and is present even when crypto configuration is not present.

  Workaround: There is no workaround.

  Further Problem Description: The output of **show policy-map type inspect zone-pair session** suggests that for single traffic stream (RDP stream) two sessions are created. One session is in half open state the other is fully established. By default the idle-timeout for half-open session is 30 sec, so after 30 seconds the half-open session is deleted and along with that it also deletes the established session.

  For both match protocol and match access-group based inspection, when inspecting TCP based protocols, inspection mechanism creates duplicate sessions.

- CSCtc82516

  Symptoms: The inbound ACL applied on the GRE tunnel interface is bypassed.

  Conditions: The symptom is observed when CEF switching is turned on. The crypto ACL encrypts all traffic going through this GRE tunnel. The ACL is trying to filter out some specific host, and is applied inbound.

  Workaround: There is no workaround.

- CSCtc87330

  Symptoms: Periodically, you may get bad “getbuffers” in “IP Input” process.

  Conditions: The symptom is observed when running traffic overnight.

  Workaround: There is no workaround.

- CSCtc90459

  Symptoms: Inbound ACL is not working properly. It does not allow packets to pass that should.

  Conditions: The symptom is observed when you configure “input access list” to allow voice packets (SIP protocol). If you apply the following configuration on the router the voice packets will get dropped:

```
access-list 101 permit udp host 85.38.230.34 eq 5060 host 85.34.23.74
access-list 101 permit udp host 85.38.230.34 host 85.34.23.74 range 16384 32767
```

Workaround: Use “log” keyword at the end of the ACL.

- CSCtd02018

  Symptoms: Unable to pass traffic.

  Conditions: The symptom is observed with IPv6 DMVPN (tunnel protection), IPv6 inspect, and IPv6 CEF.

  Workaround 1: Use running in process.

  Workaround 2: Take the tunnel protection off.

  Workaround 3: Use the **no ipv6 inspect** command.

- CSCtd10824

  Symptoms: Switch occasionally crashes when power is turned off on an interface using the **energywise** command.

  Conditions: It occurs when recurrences are already set on the interface and if they are in effect.

  Workaround: Use “energywise” queries to set levels on the interface. Queries is a more robust and time-saving technique to set levels on interfaces in bulk.

- CSCtd12681

  Symptoms: Misordered packets occur among packets which belong to the same class-map when shaping becomes active on the tunnel interface.

  Conditions: The symptom is observed under the following conditions:

  1. IPSec must be enabled, either on tunnel or physical interface.
  2. Shaping (with either **bandwidth** or **priority** command) must be applied on tunnel interface.
  3. There should be enough traffic to trigger shaping.
  4. On a Cisco 7200 series router, VAM2+ or software encryption engine has to be used.

  Workaround: Use Cisco IOS Release 12.3(14)T2 or earlier, and crypto map on physical interface instead of tunnel protection on tunnel interface for IPSec encryption.

  Alternate Workaround: Use Cisco IOS Release 12.4(20)T or later where HQF QoS is introduced. HQF QoS does not have the issue regardless of hardware or software configurations.

- CSCtd12700

  Symptoms: A GM pseudotime gets desynchronized after re-registering or at initial registration.

  Conditions: The symptom is observed with GETVPN when Time Based Anti-Replay (TBAR) is enabled. After establishing phase I, the GM is supposed to get the KEK and TEKs. If there is packet drop (most of the time this message is fragmented across multiple frames), then the router is not able to reassemble the packet. Then IKE will resend this message later but the pseudotime has not been recalculated.

  Workaround: Disable TBAR or use a very large window (greater than 30 seconds).

- CSCtd23069

  Symptoms: Crash due to SegV exception after configuring “ip virtual-reassembly”.

  Conditions: The symptom is observed on a Cisco 7206VXR router configured as LNS that is running Cisco IOS Release 12.4(15)T7 and Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd25879

  Symptoms: When upgrading to Cisco IOS Release 12.4(15)T10, IPSec client can connect to a Cisco 7301 router but when the IPSec client disconnects, the router keeps the IPSec session UP. It is not possible to connect to the 7301 IPSec concentrator again.

  Conditions: The symptom is observed with a Cisco 7301 router that is running Cisco IOS Release 12.4(15)T10.

  Workaround 1: Disable/enable crypto map:

  ```
  interface gig 0/0
  no crypto map
  crypto map map name
  ```

  Workaround 2: Remove access-list and apply again:

  ```
  interface gig 0/0
  no ip access-group ACL NAME in
  ip access-group ACL NAME in
  ```

  Workaround 3: Reload the router.

- CSCtd28809

  Symptoms: An HWIC-3G may not work on some sites. The following error messages may be seen:

  ```
  CELLWAN-2-HEART_BEAT_TIMEOUT: No heart beat signal from Cellular0/1/0
  HWIC_CELL-1-MODEM_ACK_FAIL : [Cellular0/1/0] Modem Ack not received
  ```

  Conditions: The symptom is observed on a Cisco 1841 router.

  Workaround: Use the following steps:

  - Power off the router.
  - Disconnect the cable from the antenna.
  - Power on the router.
  - Wait until you have the prompt on your console or when you can access it via telnet.
  - Screw antenna cable back.

  At this point, communication should be possible.

- CSCtd34862

  Symptoms: The command **show policy-map interface** *multilink1*, shows that transmitted packets/bytes counter is incorrectly increasing for DSCP values that is not being matched in the class map on the Cisco 2821 platform.

  Conditions: The symptom is observed on a Cisco 2821 router.

  Workaround: There is no workaround.

- CSCtd37738

  Symptoms: The symptoms are as follows:

  - Phone A calls Phone B.
  - Phone B is call-forwarded to a cell phone C.
  - Cell phone C is ringing.
  - Phone A does not hear ring back.

  Conditions: The symptom is observed when the CCM is between CUBE and VGW.

  Workaround: There is no workaround.

- CSCtd42508

  Symptoms: PVDM3 DSP might crash under excessive T38 fax call failures.

  Conditions: This symptom is observed under network packet loss conditions.

  Workaround: There is no workaround.

- CSCtd57788

  Symptoms: A dynamic IP ACL is created when a session comes up and is together with the policy private route created according to the "Ascend-Private-Route" downloaded from the user profile. When the session goes down, the route is cleared but the dynamic ACL is not cleared:

```
dge2-18#sh ip access-lists dynamic
Extended IP access list pbr#1
    10 permit ip any host 10.1.1.1 (5 matches)
Extended IP access list pbr#2
    10 permit ip any host 10.1.1.1 (5 matches)
Extended IP access list pbr#3
    10 permit ip any host 10.1.1.1 (25 matches)
Extended IP access list pbr#4
    10 permit ip any host 10.1.1.1 (25 matches)
Extended IP access list pbr#5
```

  Conditions: The symptom is observed with routes downloaded from the radius server.

  Workaround: There is no workaround.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

  Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

  Workaround: There is no workaround.

- CSCtd61443

  Symptoms: GETVPN key server may crash after modifying group ACL.

  Conditions: This is seen on Cisco router with Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd64434

  Symptoms: FastEthernet port on a NM-2FE2W stops processing incoming packets.

  Conditions: The symptom is observed with an NM-2FE2W Network Module.

  Workaround: There is no workaround.

- CSCtd73843

  Symptoms: A Cisco 1801 router flaps intermittently.

  Conditions: The symptom is observed with a third-party vendor IP DSLAM.

  Workaround: There is no workaround.

- CSCtd75189

  Symptoms: Continuous error message similar to the one below are recorded on voice gateway:

```
SYS-2-INPUTQ: INPUTQ set, but no IDB, ptr=6818DA34, -Traceback=
```

Conditions: The symptom is observed on a voice gateway that is running Cicso IOS Release 12.4(24)T2.

Workaround: There is no workaround.

- CSCtd79357

  Symptoms: Issuing the **show license call-home pak** *xxx* command at TCL mode will crash system. For example:

  ```
  Router(tcl)#exec "show license call-home pak PAKString"
  ```

  Conditions: The symptom is observed upon issuing the **show license call-home pak** *xxx* command at TCL mode.

  Workaround: There is no workaround.

- CSCtd86638

  Symptoms: Router reports the following error messages,

  ```
  - %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for CCE 7tuple dyn  No
  memory available -Process= "Chunk Manager", ipl= 3, pid= 1 -Traceback=
  0x232BCB84z 0x232BCB68z
  - %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for Firewall State. No
  memory available -Process= "Chunk Manager", ipl= 3, pid= 1 -Traceback=
  0x232BCB84z 0x232BCB68z
  ```

  Conditions: The symptom is observed when the router has high sessions, i.e.: connections/second coming in for prolonged period of time.

  Workaround: There is no workaround.

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd90367

  Symptoms: Router crashes every 2-3 days with URLF feature. The error message shows memory leak issues.

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(24)T2, with URLF features on the device.

  Workaround: There is no workaround.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCtd95386

  Symptoms: An IPSec tunnel can be torn down if the router receives a replayed QM (Quick Mode) packet.

  Conditions: This is only a problem when a replayed QM packet is received on an IPSec endpoint.

Workaround: There is no workaround.

- CSCtd97164

  Symptoms: LLQ packet drops on an ATM interface.

  Conditions: The symptom is observed when having QoS under an ATM interface. Packet drops are seen under a class with “priority”, even though they have not reached the value configured. It does not matter if it is percent or absolute value.

  Workaround: There is no workaround.

- CSCte01576

  Symptoms: CPU goes up to 99 percent when TRP is used for making voice calls with 50 SCCP and 50 SIP endpoints.

  Conditions: The symptom is observed when STUN inspection is enabled on the firewall for media traversal.

  Workaround: Use SIP or SCCP inspection.

- CSCte02973

  Symptoms: Routing protocols like EIGRP may be dropped in the global table.

  Conditions: The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

  Workaround: Enable “ip multicast routing” and create a loopback interface with “ip pim sparse-mode” enabled.

  Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

  However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.

- CSCte03048

  Symptoms: Fragmentation does not occur on a Cisco 7200 series router.

  Conditions: The symptom is observed when FR encapsulation is configured and fragmentation is enabled. Now do a **wr mem** and reload.

  Workaround: Perform an OIR on the PA.

- CSCte07401

  Symptoms: Normal mode GD fails with tracebacks when you execute the **show memory debug leak chunks** command.

  Conditions: This symptom is seen when you check for memory leaks after clearing an L2TP session.

  Workaround: Wait for all sessions to tear down and then check for leaks.

- CSCte07862

  Symptoms: DSP crashes due voice card shutdown, with an intermittent CPHI error.

  Conditions: The symptom is observed when the phones are connected to PBX. Users dial 5XXXX from the phone. The pattern then changes to 895XXX between PBX and the Cisco router. Over the IP, the call is transferred to 2821 voice card gateway where there is another PBX.

  Workaround: There is no workaround.

- CSCte12104

  Symptoms: Crash at startup with the following error message:

  %SYS-6-STACKLOW: Stack for process ATM Periodic running low, 0/9000

  Conditions: The symptom is observed when QoS policy is applied on an ATM interface. There is no specific trigger.

  Workaround: There is no workaround.

  Further Problem Description: This issue may not be widely hit as it is difficult to reproduce.

- CSCte16755

  Symptoms: In an IPSec GetVPN setup, multicast endpoints are not reachable/pingable.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(15)T12.

  Workaround: There is no workaround.

- CSCte17284

  Symptoms: A router may unexpectedly reload due to software forced crash because of chunk memory corruption.

  Conditions: The crash appears to happen when using the clientless web proxy method. The crash is triggered by accessing a webpage through the SSL VPN with a URL longer than 1009 characters long.

  Workaround: If possible, redesign the website to use URLs of 1009 characters or shorter.

- CSCte17560

  Symptoms: Offered rate in QoS class shows unusually high values

  Conditions: The symptom is observed when service-policy is applied on a multilink interface.

  Workaround: There is no workaround.

- CSCte18124

  Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024”.

  Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.

  Workaround: Create ATM PVC without “atm vc-per-vp 1024”.

- CSCte27805

  Symptoms: Self ping on a dialer interface fails when it is over a PPPoE link.

  Conditions: The symptom is observed when the dialer interface is up and its underlying interface is PPPoE.

  Workaround: There is no workaround.

- CSCte39643

  Symptoms: A router crashes.

  Conditions: The symptom is observed with OER and EIGRP configurations.

  Workaround: There is no workaround.

- CSCte41231

  Symptoms: Router crashes when unconfiguring “iphc profile”.

Conditions: The symptom is observed when “iphc profile” is configured on dialer interfaces. Then “iphc profile” is not properly removed from the dialer followed by a “no iphc-profile” done globally.

Workaround: There is no workaround.

- CSCte51958

  Symptoms: Large amount of memory leaks are seen at Expression Handler.

  Conditions: The symptom is observed while doing an SNMP set and walk on expExpressionEntry table.

  Workaround: There is no workaround.

- CSCte53097

  Symptoms: When the IP address of the HA is set to the VIP address of HSRP, end-to-end connectivity will be lost. Tunnel keepalives from the mobile node fail and the bindings are deleted from HA.

  Conditions: This is seen in Cisco IOS Release 12.4(23) when using the HA behind a NAT device and the translated (inside) IP of the HA is set to the HSRP VIP address.

  Workaround: Configure a loopback interface (does not have to be routed) with the same outside (public) IP that the mobile node connects to. This is the outside IP defined in the NAT rule on the NAT device.

- CSCte53275

  Symptoms: A Cisco 1841 router running GETVPN with Cisco IOS Release 15.0(1)M may receive the following error:

  ```
  %SYS-2-SHARED: Attempt to return buffer with sharecount 0, ptr= 667BAEA4
   -Process= "Crypto Support",
    ipl= 4, pid= 225 -Traceback= 0x6162E284z 0x631AB270z 0x63342F14z 0x62757380z
   0x62757364z
  ```

  Conditions: The exact trigger has not yet been determined.

  Workaround: There is no workaround.

- CSCte54807

  Symptoms: Configuring PVC with Cisco IOS Release 15.0(1)M1 brings up a virtual-access interface, right after sending the ConfReq, even if there is no reply.

  Conditions: The symptom is observed when using a PPPoA setup on Cisco IOS Release 15.0(1)M1. It is seen only if some unused ATM PVCs are present at one end with the PPP configurations applied on them.

  Workaround: Use Cisco IOS Release 12.4(24)T2.

- CSCte57140

  Symptoms: Lawful intercept does not work for PSTN hairpinned calls. Softswitch redirects the incoming PSTN call to the telco. Although CRCX comes with “L: e:off” and NOT with “L: e:off,nt:LOCAL”, the DSPs are still dropped for the first call.

  Conditions: The symptom is observed with a Cisco AS5350XM that is running Cisco IOS Release 12.4(23).

  Workaround: There is no workaround.

- CSCte58825

  Symptoms: There is a crash upon conducting an snmpwalk from “enterprise mib oid 1.3.6.1.4.1”.

Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 12.2(33)XNE.

Workaround: Configure SNMP view to exclude ipSecPolMap as follows:

```
snmp-server view view name iso included
 snmp-server view view name ipSecPolMapTable excluded
 snmp-server community community string view view name RO
```

- CSCte61495

  Symptoms: The following messages are seen with tracebacks:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process
  = Exec. %SYS-2-INTSCHED: 'suspend' at level 3
  -Process= "Exec", ipl= 3, pid= 128,
  ```

  Conditions: The symptom is observed when a large ACL is configured for the service-policy. This happens only under ATM subinterfaces.

  Workaround: Use small sized ACLs for the service-policy.

- CSCte61528

  Symptoms: Router crashes when configuring "tftp hostname" with a longer name.

  Conditions: The symptom is observed with a Cisco 7200 series router loaded with the 151-0.25.T image.

  Workaround: There is no workaround.

- CSCte62190

  Symptoms: A router crashes when the RSA key is generated with redundancy option and then the RSA key pair is deleted using the **crypto pki zeroise rsa** command.

  Conditions: The symptom is observed with a router loaded with the c7200-adventerprisek9-mz.151-0.25.T image.

  Workaround: There is no workaround.

- CSCte63156

  Symptoms: Router hangs and crashes when a DHCP pool configured with "origin aaa subnet" is removed.

  Conditions: The symptom is observed when pool is configured with "origin aaa subnet ..." and without unconfiguring this command, the pool is deleted with the **no ip dhcp pool** command. Also missing is "aaa accounting" with "default method-list" from global configuration.

  Workaround: Globally configure "aaa accounting" with "default method-list" ("aaa accounting network default").

- CSCte63390

  Symptoms: Memory leak seen under CCH323_CT process. The leak leads to a low memory condition and malloc failures under the processor memory pool.

  Conditions: Unknown at this point.

  Workaround: There is no workaround.

- CSCte63404

  Symptoms: Fax passthrough between H.323 gateway (registered with CUCM 7.1.3) fails.

  Conditions: The symptom is observed when CUCM 7.1.3 does the call control for the H.323 gateway. The fax call from GW1 to GW2 gets disconnected as soon as the call is established.

Workaround: There is no workaround.

- CSCte64544

  Symptoms: Calls fail following hook flash on a T1-CAS circuit.

  Conditions: The symptom is observed following outbound calls over a T1-CAS E&M, and after a hookflash.

  Workaround 1: Reorder circuits in CUCM RG.

  Workaround 2: Perform a shut/no shut on the T1-CAS controller.

- CSCte64621

  Symptoms: VSA stops passing traffic after the first IPSec rekey.

  Conditions: The symptom is observed VSA specific.

  Workaround: There is no workaround.

- CSCte68288

  Symptoms: Spurious memory access is seen when a set of configurations is placed under “crypto pki trustpoint *name*”.

  Conditions: The symptom is observed when the router is loaded with the c7200-adventerprisek9-mz.151-0.25.T image.

  Workaround: There is no workaround.

- CSCte68795

  Symptoms: High CPU utilization is observed with IP NBAR protocol discovery.

  Conditions: The symptom is observed when enabling “ip nbar protoocol discovery”.

  Workaround: WINMX PDLM needs to be reverted back to the previous version.

- CSCte70409

  Symptoms: A crash seen when running TCL scripts/testcases testing COOP feature of GETVPN.

  Conditions: The symptom is observed when running multiple testcases at a time as part of internal testing.

  Workaround: There is no workaround.

- CSCte75220

  Symptoms: Router crashes when configuring “key-string www” in key chain mode.

  Conditions: The symptom is observed when configuring “key-string www” in key chain mode via console, and when key chain is unconfigured in the vty mode.

  Workaround: There is no workaround.

- CSCte76092

  Symptoms: Cisco 880 series router does not write crashinfo.

  Conditions: The symptom is observed with a Cisco 880 series router.

  Workaround: Connect a device to monitor the console.

- CSCte76513

  Symptoms: If ZBF and WAAS are configured on a router, you may see drop logs similar to the following:

  ```
  %FW-6-DROP_PKT: Dropping tcp session x.x.x.x y.y.y.y due to No zone-pair between zones
  with ip ident 0
  ```

```
%FW-6-DROP_PKT: Dropping http session x.x.x.x y.y.y.y on zone-pair admin-to-wan class
admin due to Invalid Flags with ip ident 0
```

Conditions: The symptom is observed if ZBF and WAAS are configured on a router.

Workaround: There is no workaround.

- CSCte76760

  Symptoms: A router acting as a voice gateway may unexpectedly reload due to bus error.

  Conditions: The symptom is observed when the gateway is experiencing a low memory problem leading to seeing SYS-2-MALLOCFAIL errors.

  Workaround: Resolve the low memory problem.

- CSCte78204

  Symptoms: Vaccess interface does not come up.

  Conditions: The symptom is observed when **clear interface virtual-access #** is issued on a Cisco 7200 series router and when LFIoFR is configured.

  Workaround: Perform a shut/no shut on the serial member.

- CSCte82086

  Symptoms: A Cisco 1900 series or Cisco 2900 series router sometimes does not respond to “break” on the RJ45 console or the USB console.

  Conditions: The symptom is observed on a Cisco 1900 series or Cisco 2900 series router.

  Workaround: Press “break” on the terminal keyboard couple times after seeing “program load complete,...” message, in order to put the router into ROMMON.

- CSCte85781

  Symptoms: Policy with more bandwidth then physical and tunnel interface bandwidth is attached on tunnel interface.

  Conditions: The symptom is observed with a Cisco 7200 series router and Cisco IOS interim Release 15.1(00.26)T.

  Workaround: There is no workaround.

- CSCte85818

  Symptoms: Priority burst on **sh policy-map int** shows more than the burst value defined on the command syntax range.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(00.26)T.

  Workaround: There is no workaround.

- CSCte89130

  Symptoms: Router experiences a memory leak.

  Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **sh mem alloc total** command).

  Workaround: There is no workaround.

- CSCte89436

  Symptoms: Router crashes.

  Conditions: The symptom is observed when encapsulation is changed from from “frame-relay” to “hdlc”.

Workaround: There is no workaround.

- CSCte89787

  Symptoms: A Cisco ASR 1000 crashes after the Segment Switch Manager (SSM) reports that an invalid segment has been detected:

  ```
  %SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment class.
  ```

  The crash follows this message.

  Conditions: The symptom is observed on a Cisco ASR 1002 that is running Cisco IOS Release 12.2(33)XND1. The crash is caused by a NULL pointer de-reference following the “no segment class” error. The error itself is not fatal and the crash should have been avoided.

  Workaround: There is no workaround.

- CSCte90278

  Symptoms: Watchdog crash observed on a Cisco 3845 router.

  Conditions: The symptom is observed with a Cisco 3845 router with frame relay encapsulation on the dialer and WIC-1DSU-T1-V2 serial interfaces.

  Workaround: There is no workaround.

- CSCte91471

  Symptoms: Clock synchronization with the NTP server could be lost for several hours if router (NTP client) runs NTPv4.

  Conditions: The symptom is observed if the router clock is reset (for example: by using the **clock set** exec command). The router then takes a long time to synchronize again.

  Workaround: There is no workaround. The clock will automatically synchronize after few hours.

- CSCte91782

  Symptoms: Cannot unconfigure “crypto pki server <>” when “crl” is configured.

  Conditions: The symptom is observed on a router loaded with Cisco IOS interim Release 15.1(1.1)T.

  Workaround: There is no workaround.

- CSCte91990

  Symptoms: A Cisco 3845 router with HWIC-4ESW is flooding packets to all interfaces even back across the same interface.

  Conditions: The symptom is observed when sending to a packet with a mulitcast MAC and unicast IP address.

  Workaround: There is no workaround.

- CSCte93792

  Symptoms: Virtual access bound to an ATM interface does not come up.

  Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.

  Workaround: There is no workaround.

- CSCte94221

  Symptoms: PPP connection over CDMA link is flapping.

  Conditions: The symptom is observed when using Cisco IOS Release 15.0M.

Workaround: There is no workaround.

- CSCte95301

  Symptoms: Memory leak in proxy authentication scenario, when authentication fails.

  Conditions: The symptom is observed when HTTP proxy authentication is used.

  Workaround: There is no workaround.

- CSCte98702

  Symptoms: When using NAT, "%SYS-3-INVMEMINT and %SYS-2-MALLOCFAIL" are printed to the console and no traffic passes.

  Conditions: The symptom is observed when NAT is configured.

  Workaround: There is no workaround.

- CSCtf00427

  Symptoms: A router may experience a severe memory leak issue when the following command is configured:

  privilege exec level *level* **show ip ospf neighbor**

  Conditions: The symptom is observed when running Cisco IOS Release 12.2(33)XNE or 12.2(33)XNE1. The issue is not platform dependent.

  Workaround: Reload the router.

- CSCtf03436

  Symptoms: A two-level policy attached on a multilink interface is getting detached when the interface undergoes a shut/no shut.

  Conditions: The symptom is observed with a two-level policy configured with shaper/bandwidth percent. It is seen on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCtf03850

  Symptoms: The **configure replace/terminal revert** commands are not working.

  Conditions: The symptom is observed on a Cisco 2811 router that is running Cisco IOS Release 15.0(1)M and a Cisco 877W router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtf04132

  Symptoms: Tracebacks are seen on an L2TP Network Server (LNS) after new session is established.

  Conditions: The symptom is observed on an LNS.

  Workaround: There is no workaround.

- CSCtf05429

  Symptoms: Serial interface flap is seen on a Cisco 7200 series router.

  Conditions: The symptom is observed when controller 1/1 is configured as unchannalized and then you do a sweep ping.

  Workaround: There is no workaround.

- CSCtf07474

  Symptoms: TCP sessions fail to establish between two routers over an IPSEC VPN tunnel after an EZVPN client session has been established and torn down to the two routers. The TCP sessions could be a telnet or H.323 sessions that terminate and originate between the two routers. Logs show:

  ```
  %FW-6-DROP_PKT: Dropping tcp session 192.168.10.1:58553 192.168.20.1:23 due to
  Invalid Segment with ip ident 35331 tcpflags 0x5010 seq.no 2978402186 ack 1370657297
  ```

  Conditions: The symptom is observed under the following conditions:

  - Two routers setup with IPSEC point-to-point VPN.
  - Using Cisco IOS Release is 15.0(1)XA or later.
  - Both routers are setup as EZVPN servers.
  - An EZVPN session has been established to one of the routers and has been disconnected.

  Workaround:

  - Always keep an EZVPN client session up to the router.
  - Remove and add **ip inspect** on WAN interface after EZVPN session has been disconnected.

- CSCtf08645

  Symptoms: A Cisco 2800 series router crashes.

  Conditions: The symptom is observed with the c2800nm-advipservicesk9-mz.124-24.T2 image. The crash is most likely to occur when a hardware IDS module is present.

  Workaround: There is no workaround.

- CSCtf09228

  Symptoms: A router may crash.

  Conditions: The symptom is observed on a Cisco 1802W router that is running Cisco IOS Release 15.0(1)M1, after bringing up a second PPPoE connection.

  Workaround: There is no workaround.

- CSCtf11642

  Symptoms: A router may crash due to a bus error.

  Conditions: The symptom has been observed on a Cisco 1841 router that is running Cisco IOS Release 12.4(24)T2, with IOS Firewall configured.

  Workaround: There is no workaround.

- CSCtf13014

  Symptoms: DNS server on a router first consults with its next-level DNS servers when servicing queries for its primary zone.

  Conditions: This symptom only happens when next-level (parent) DNS servers are configured on the router.

  Workaround: There is no workaround.

- CSCtf13408

  Symptoms: Router crashes when using “config replace” to remove “sccp” configurations such as “associate ccm” and “associate profile” in the “sccp ccm group” sub-mode.

Conditions: This symptom occurs when SCCP is enabled and configured with “associate ccm” or “associate profile”, and “config replace” is used to roll back the router configuration to a state where “associate ccm” or “associate profile” for “sccp ccm group” does not exist, i.e. to remove those configuration commands after rollback.

Workaround: The user can manually change the configuration instead of using “config replace” as follows:

1. Use the command **show archive config differences** [**flash:** | *file path*] to determine the difference between the running-config and the saved config (in flash: or by valid file path);
2. Manually change the running config line-by-line through the differences shown in the above command output.

- CSCtf18077

  Symptoms: A CME router may unexpectedly reload due to bus error when a UCCX unregisters from the CME.

  Conditions: This symptom is seen when the UCCX unregisters from the CME.

  Workaround: There is no workaround.

- CSCtf19461

  Symptoms: IP address is not leased out to the client from server.

  Conditions: Configuring vpn sub-option at the interface level on relay

  Workaround: There is no workaround.

- CSCtf19572

  Symptoms: Crash occurs while unconfiguring “interface ATM0/1/0.1 point-to-point”.

  Conditions: This symptom is observed while unconfiguring “interface ATM0/1/0.1 point-to-point”.

  Workaround: There is no workaround.

- CSCtf22064

  Symptoms: Invalid configuration is attaching on frame relay map class

  Conditions: This symptom is observed on a Cisco 7200 platform on Cisco IOS interim Release 15.1(1.3)T

  Workaround: There is no workaround.

- CSCtf22377

  Symptoms: A Cisco 2851 reboots due to bus error, packets (skinny) leaking

  Conditions: This crash is due to a buffer leak in the small buffers

  Workaround: There is no workaround.

- CSCtf23119

  Symptoms: On a connection trunk circuit that has it voip dial peers configured for dtmf-relay rtp-nte, dtmf stops working, where it is not heard on the receiving tdm circuit. With debug voip rtp session name-event enabled you still see rtp-nte debugs being received on the terminating side gateway, but no digits are heard on the tdm side out of the dsp.

  Workaround: A shut / no shut of one of the voice ports will drop and reconnect the connection trunk circuit and dtmf-relay rtp-nte will again work.

- CSCtf25009

  Symptoms: Multicast traffic sent out of a GE-DCARD-ESW on a NM-16ESW is process-switched, instead of being fast-switched.

  Conditions: This symptom is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(25b).

  Workaround: Use the onboard Gigabit interface.

- CSCtf25131

  Symptoms: Router crashes.

  Conditions: This symptom is observed when a large number of ISG sessions [27K or more] go down simultaneously while there is a CPUHOG on the box. Check for memory leaks using the **sh mem debug leaks chun** command.

  Workaround: Do not try to check for memory leaks in case there is a CPUHOG on the box.

- CSCtf25508

  Symptoms: Customers are not able to remove isakmp profiles followed by the error msg "% Profile is applied to Virtual-Access2-head-0/65536 and possibly other crypto maps".

  Note where 2 is in the Error msg will differ based on the customers configuration.In the above message Virtual-Access 2 is reference because the VTI number in this case was 2.

  This also keeps many stale dynamic crypto map entries without any valid ipsec sa or virtual access interface.

  Conditions: This symptom is seen when using VTI with EZVPN and only seen in Cisco IOS Release 12.4(24)T.

  Workaround: Reload the Router to release hung Virtual-Access Sessions

- CSCtf25886

  Symptoms: The following messages are observed on the console:

  ```
  028970: Feb 24 18:58:34.565: %C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors
  available on slot 5 dsp 13.

  028971: Feb 24 18:58:39.621: %C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors
  available on slot 3 dsp 17.

  028972: Feb 24 18:58:44.629: %C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors
  available on slot 3 dsp 17.
  ```

  The RST (ReSeT) counter column in the output of the **show voice dsp detail** command will show non-zero values for some Digital Signal Processor (DSP) IDs, indicating that a DSP has reset itself.

  Conditions: This behavior may be observed on a Cisco Voice GateWay that is installed with PVDM2 C5510-based DSP cards: PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-48, PVDM2-64, and AS5X-PVDM2-64, and configured for TDM-IP Voice Services. At present this symptom has been observed with Cisco IOS Release 12.4(15)T12 and default DSP firmware version 9.4.12, as well as when DSPware 9.4.10 or 9.4.11 is used in place of 9.4.12.

  Workaround: Lab reproduction work has demonstrated that superseding the default DSPware in Cisco IOS 12.4(15)T12 with DSPware version 9.4.9 or earlier constitutes a stable combination of Cisco IOS and DSPware.

- CSCtf27324

  Symptom: s Ping from a CPE which is doing PPP to the ip address of the LNS router that terminates that PPP call fails. PPP has been opened, and IPCP has negotiated an IP address. Ping from the LNS back to the CPE works fine. Between the LAC and the LNS there is a PPP multilink bundle.

Conditions: The issue happens only when we have a plain PPP call from a client (ISDN modem or dial up modem which is doing PPP). In addition the physical connectivity between the LAC and the LNS is PPP multilink.

Workaround: Disable cef on the physical interface between the LAC and the LNS. If the CPE is doing PPP multilink ping works fine.

Further Problem Description: The issue seems to be specific with the forwarding of the packets through the PPP multilink bundle that exists between the LAC and the LNS.

- CSCtf28796

  Symptoms: With async_dialer interface type, PPP fails.

  Conditions: This issue is seen only with async_dialer interface type. There is no issue with async_legacy and async_virtual interface types.

  Workaround: There is no workaround.

- CSCtf32094

  Symptoms: Traffic drops on the bundle interface with input error.

  Conditions: This symptom occurs when one member link is removed.

  Workaround: There is no workaround.

- CSCtf32916

  Symptoms: Incoming SIP call forwarded to external destination via SIP trunk will be dropped after negotiated session time expires.

  Conditions: This symptom is seen in Cisco IOS Release 12.4(24)T1 with forwarded SIP-SIP calls and session timer negotiated (RFC 4028). It is not seen in Cisco IOS Release 12.4(11)XW9.

  Workaround: -Disable or increase session timer on SIP trunk(s).

- CSCtf33270

  Symptoms: Router crashes while giving shutdown under config-nxg-neigh-svc mode.

  Conditions: This symptom is seen on a Cisco 7200 router that is loaded with Cisco IOS Release 15.1(1.4)T image.

  Workaround: There is no workaround.

- CSCtf34183

  Symptoms: Secondary CM fails to register.

  Conditions: This symptom is observed after correcting the user name.

  Workaround: There is no workaround.

- CSCtf35006

  Symptoms: We have two jobs in SNMP job Q. Try to destroy the jobs and console hangs.

  Conditions: This symptom is seen when preparing multiple license action entries and then let them execute immediately.

  Workaround: There is no workaround.

- CSCtf36117

  Symptoms: Crash occurs when executing the s**how crypto session brief** command with multiple IKIEv2 tunnel connections

Conditions: The test scenario involves setting up as much as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established, and the CLI is trying to list down the sessions. This problem is reproducible at will.

Workaround: There is no workaround.

- CSCtf36285

  Symptoms: Secondary link ias not dialed after the expiry of the initial route-check timer

  Conditions: The failure is seen only in Cisco IOS Release 12.4(24)T3.

  Workaround: There is no workaround.

- CSCtf40731

  Symptoms: Routing is formed when PIRO and OER generates static route works together.

  Conditions:

  1. PIRO generates more specific prefix for the static route it created.
  2. OER generates static route redistributed into other IGP protocol in order to get traffic.

  Workaround: There is no workaround.

- CSCtf41515

  Symptoms: There is an end-to-end ping failure.

  Conditions: This symptom is seen with the following topology:

  ```
  7200-a <------------------> 3845 <------------------> 7200-b
  ```

  After “frame-relay payload-compression” is removed on Cisco 7200-a and Cisco 3845, Cisco 3845 is able to ping Cisco 7200-a, but Cisco 7200-b is not able to ping Cisco 7200-a.

  Workaround: There is no workaround.

- CSCtf45586

  Symptoms: GW is not playing the remote ringback tone when 180 with SDP is received.

  Conditions: This symptom occurs when switching from local ringback tone to remote ringback tone.

  Workaround: There is no workaround.

- CSCtf47094

  Symptoms: After call connects between Remote phone and HQ, call either has no way or one way audio. Error is observed on the remote CISCO881.

  ```
  *Feb 24 23:30:25.675: %FW-6-DROP_PKT: Dropping tcp session 172.17.10.1:2000
  172.16.20.101:50575 on zone-pair ccp-zp-out-self class icmp-self due to Invalid Flags
  with ip ident 0
  ```

  Conditions: This only happens if the remote 79xx phone is running 8.x Phone firmware. Remote phone needs to be connected back to HQ via ZBFW and EZVPN

  ```
  CISCO881 using 15.0.1.M1

  CME3825 using 15.1.1.XB

  CP-7940 using P00308000500
  ```

  Topology:

  ```
  SCCP_7940 Ph1--CISCO881--ZBFW/EZVPN--ASA5520--CME3825--IP phone/PSTN Ph2
  ```

  Workaround: Downgrade phone firmware to a 7.x release.

- CSCtf47335

  Symptoms: Wrong typedef version is returned.

  Condition: On getTypedefs CT, Cisco IOS returns a typedefVerion “2008-08-01”. This is a wrong version with some undefined entries. Due to this, the signature parsing is failing in CCP.

  Workaround: There is no workaround.

- CSCtf47396

  Symptoms: Router may crash when a service-policy configured with bandwidth is removed from an interface.

  Conditions: This issue is seen with Cisco 7200 router that is loaded with Cisco IOS interim Release 15.1(1.5)T image.

  Workaround: There is no workaround.

- CSCtf48094

  Symptoms: UUT crashes for ftp traffic with debugs enabled for IPv6 inspection.

  Conditions: Crash is seen only with Legacy Firewall for IPv6 inspection.

  Workaround: There is no workaround.

- CSCtf48179

  Symptoms: When using authentication header only (no encryption over the tunnel) around 30% of outgoing traffic is dropped due to incorrect IP header checksum.

  Conditions: This symptom is occurring on 2 different Cisco 2901 routers that are running Cisco IOS Release 15.0(1)M1. AH is configured via “crypto ipsec transform-set AH-MD5 ah-md5-hmac”. This problem occurs only on high latency link (via sitcom).

  Workaround: Encrypt the packets by changing the transform-set from ah-md5-hmac to esp-3des esp-sha-mac.

- CSCtf48612

  Symptoms: Active learnt forwarder for GLBP should never timeout with a listening forwarder present.

  Conditions: Configure GLBP on two routers and force both Active forwarders to be on the same router.

  Router1 configs:

  track 1 stub-object
  interface *interface name*
  ip address *ip address ip mask*
  glbp *group number* **ip** *virtual ip address*
  glbp *group number* **timers redirect** *interval value timeout value*
  glbp *group number* **weighting track** *track number* **decrement** *decrement value*

  Router2 configs:

  interface *interface name*
  ip address *ip address ip mask*
  glbp *group number* **ip** *virtual ip address*
  glbp *group number*
  timers redirect *interval value timeout value*

  Workaround: There is no workaround.

- CSCtf49950

  Symptoms: Router that is configured with IPS experiences memory leak.

  Conditions: This symptom occurs when IPS is configured.

  Workaround: There is no workaround.

- CSCtf50867

  Symptoms: Router reloads at iprouting_is_hdvrf_idb.

  Conditions: This symptom occurs when configuring pri-group nfas_d with Cisco IOS Release 15.1(01.05)T.

  Workaround: There is no workaround.

- CSCtf50992

  Symptoms: MS Callback fails with local authentication.

  Conditions: This issue is seen when we configure local authentication. There is no issue with RADIUS authentication.

  Workaround: There is no workaround.

- CSCtf51156

  Symptoms: On a Cisco router that is running ISIS with 1 second as hello interval, Compact flash removal and insertion may result in ISIS neighborship flap.

  Conditions: This issue is observed when ISIS is configured with 1 second as hello interval.

  Workaround: There is no workaround.

- CSCtf51690

  Symptoms: Router will crash when a packet with out of bound featureIndex is sent to CME.

  Conditions: This symptom occurs when malformed packets are being sent to CME with out of bound featureIndex values in fStationFeatureStatReqMessage.

  Workaround: There is no workaround.

- CSCtf59960

  Symptoms: DHCP pool does not assign IP add to other interface when virtual interface is configured and removed.

  Conditions: This problem is seen in Cisco 7200 series router that is loaded with Cisco IOS Release 12.4(24)T3.

  Workaround: There is no workaround.

- CSCtf62621

  Symptoms: Cannot push the FW down to the VDSL chipset on the Cisco 887V modem.

  Conditions: This symptom is observed on a Cisco 887V router with no startup-config in NVRAM.

  Workaround: “wr me” and reload the router.

Resolved Caveats—Cisco IOS Release 15.1(1)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCef82896

  Symptoms: When the user name in the authentication dialog box is left blank, the router unexpectedly reloads.

  Conditions: The symptom is observed when authenticating via the HTTP server. It is observed only when a valid user name was previously configured:

  ```
  (config)#ip http authentication local
  (config)#username <name> privilege <number> password <password>
  ```

  Workaround: Do not leave the user name blank in the authentication text box if username authentication is enabled.

- CSCsc49637

  Symptoms: If a PPPoE client session is timed out (e.g. due to a network outage), and a restart of the session is subsequently unsuccessful (e.g. because network outage persists or the PPPoE server has not timed out the prior session) and if the user then manually clears the session, then the router will no longer be able to bring up this session until a reload is performed.

  Conditions: This symptom has been observed when the PPPoE session is unexpectedly interrupted with Cisco IOS Release 12.3(8)T8 or Release 12.3(11) T5. The next feature also needs to be configured:

  ```
  pppoe-client dial-pool-number 1 dial-on-demand
  ```

  Workaround: Use the following procedure:

  1. Reload.
  2. Do not configure the DDR feature for the PPPoE session. This problem is limited to PPPoE client sessions using the DDR feature.

- CSCsc62963

  Symptoms: The interface MTU is not user configurable. When you attempt to configure “interface level command mtu,” the following message is printed:

  ```
  % Interface {Interface Name} does not support user settable mtu.
  ```

  Conditions: The symptom is observed with a 2-Port FE on a Cisco 7200 series router.

  Workaround: There is no workaround.

  Further Problem Description: The Cisco.com document entitled *MPLS MTU Command Changes* further discusses this enhancement.

- CSCsh96558

  Symptoms: A traceback may be generated during the “ipmcast_ipv6_rpf_lookup” function.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when you configure IPv6 multicast routing on both the PE router and a connected CE router, add an IPv6 address to the connected interfaces, and configure PIM sparse or PIM sparse-dense mode on both routers. The traceback is generated when the neighborship comes up after you have configured one of the interfaces as a PIM-RP.

  Workaround: There is no workaround.

- CSCsl52962

  Symptoms: The RP crashes due to a watchdog timeout of the uRPF stats process.

  Conditions: The symptom is observed when issuing the **interface range port-channel** *number - number* command.

  Workaround: There is no workaround.

- CSCsq71492

  Symptoms: A Cisco IOS device may reload with an address error or have alignment errors and tracebacks such as

  ```
  %ALIGN-3-SPURIOUS or %ALIGN-3-TRACE
  ```

  Conditions: The symptoms are most likely to occur when the TACACS+ server (ACS) sends an "authentication error" when ACS is configured, or when a request timeout occurs. There may be other AAA- or TACACS-related conditions that cause the symptom.

  Workaround: There is no workaround.

- CSCsr98707

  Symptoms: When the main ATM interface MTU has an explicit non-default value (something other than 4470), then the subinterfaces may not save (shown with the **show run** command) the explicit MTU configuration of the default (4470) even though the command is expected.

  Conditions: The symptoms are observed only for the ATM MTU value 4470. This unexpected behavior is not seen for any other value (less than or more than 4470 within allowed ATM MTU values).

  Workaround: Upon reload, manually (explicitly) configure MTU 4470. You can configure an IP MTU under the ATM interface instead of an ATM MTU.

- CSCsu50869

  Symptoms: Calls do not complete because Cisco Unified Border Element (CUBE) does not send PRACKs to all 1xx messages.

  Conditions: This symptom is observed with h.323 slow start to SIP delayed media call flow.

  Workaround: Enable fast start h.323 with an MTP in CUCM, which allows for SIP early offer. Reliable 1xx messaging can also be disabled to prevent the requirement of provisional acknowledgements.

- CSCsu78975

  Symptoms: Crash seen @adj_switch_ipv4_generic_les on a Cisco 38xx router.

  Conditions: This symptom is observed upon entering the command **no ip route 10.2.82.0 255.255.255.0 vlan1**.

  Workaround: There is no workaround.

- CSCsv00168

  Symptoms: Junk values are displayed on a Cisco router when characters or commands are entered. For example, when **show version** is entered, "h ^v^@e^@^r^@^@^@^@^@" is displayed.

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

  Workaround: There is no workaround.

  Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv03300

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

  Conditions: This symptom is observed when a CBWFQ QoS policy is attached to the onboard gigabit ethernet interface.

  Workaround: There is no workaround.

- CSCsv30540

  Symptoms: The error message `%SYS-2-CHUNKBOUNDSIB` and a traceback are seen.

  Conditions: These symptoms are observed when the **show running-config/write memory** command is entered.

  Workaround: There is no workaround.

- CSCsw15188

  Symptoms: A router running Cisco IOS may reload unexpectedly.

  Conditions: This is seen when “logging host <address> session-id” is configured. Configuring “logging host <address>” without the additional keywords will not cause the problem.

  This bug also requires certain log messages that use new lines, such as debugs from **debug isdn q931**.

  Workaround: Disable the syslog server when doing the debugs.

- CSCsw18733

  Symptoms: A Cisco 7200 router may crash while unconfiguring crypto ipsec tunnel with EzVPN client configurations.

  Conditions: This symptom is observed when crypto ipsec tunnel is configured and then unconfigured.

  Workaround: There is no workaround.

  Further Problem Description: A Cisco 7200 router crashes when unconfiguring a virtual-template of the tunnel type.

- CSCsw52855

  Symptoms: CRC and frame errors are seen if mark was used as the idle character between packets.

  Conditions: This problem occurs when using the following interface cards:

  - VWIC2-1MFT-T1/E1
  - VWIC2-2MFT-T1/E1
  - VWIC2-1MFT-G703
  - VWIC2-2MFT-G703

  Workaround: Use the following interface cards that are not affected by this problem:

  - HWIC-4T1/E1
  - HWIC-2CE1T1-PRI
  - HWIC-1CE1T1-PRI

  This is caveat has been closed.

- CSCsw62346

  Symptoms: When unsupported filter is added to global policy-map with only match-any as the filter, the router or line card might crash.

  Conditions: Occurs when global policy map is attached to an interface.

  Workaround: Detach service policy from interface before making changes.

- CSCsw76113

  Symptoms: Unable to reuse a sub-interface as main-interface.

  Conditions: Occurs when we configure **no virtual-template subinterface** when all of the Interface Descriptor Blocks (IDB) that platform supports are used as “subif-vaccess”. No more “vaccess” can be created.

  Workaround: Do not configure **no virtual-template subinterface** at run time. Check **show vtemplate** output. If there are more IDBs used by subinterface, then do not configure **no virtual-template subinterface**.

- CSCsx20147

  Symptoms: The delay value to destination computed is different between IPv4 and IPv6.

  Conditions: Occurs when EIGRP for IPv6 is configured.

  Workaround: There is no workaround.

- CSCsx26025

  Symptoms: Wireless clients are not able to ping each other after a few minutes.

  Conditions: Can occur on any of the following routers with 802.11 wireless interfaces:

  Cisco UC500, Cisco 85x, Cisco 87x, Cisco 1811, Cisco HWIC-AP

  Workaround: There is no workaround.

- CSCsx32049

  Symptoms: Traceback is observed and the system may reboot, depending on the platform.

  Conditions: The symptom is observed when the ESM filter is configured and contains an ios_config statement.

  Workaround: Remove ios_config statements from ESM filter.

- CSCsx75520

  Symptoms: Ping is not working on a Cisco router with a ctunnel interface.

  Conditions: This symptom is observed after attaching a policy map to a ctunnel interface.

  Workaround: Delete the policy map from the ctunnel interface using the **no policy-map** command and reload the router.

- CSCsx75623

  Symptoms: Tracebacks are seen when “create on-demand” is configured on a VC class and when an OIR is performed on the ATM interface.

  Conditions: This symptom occurs only if an OIR is performed when the configurations are made.

  Workaround: There is no workaround.

- CSCsx93245

  Symptoms: A Cisco router may reload after issuing the **show gatekeeper zone prefix all** command.

  Conditions: This symptom is observed on a Cisco 3825 router running Cisco IOS Release 12.4(8a).

Workaround: There is no workaround.

- CSCsy10893

  Symptoms: A Cisco router reloads occasionally after the command **show buffers leak** is repeatedly entered.

  Conditions: The symptom is observed when entering the **show buffers leak** command. It occurs only with certain patterns and scale of traffic and does not occur all the time.

  Workaround: There is no workaround.

- CSCsy19751

  Symptoms: Several chunk element leakages are seen when the **show memory debug leaks chunk** command is entered.

  Conditions: Occurs after a reboot.

  Workaround: There is no workaround. Please ignore the leaks as they are false alarms.

- CSCsy34256

  Symptoms: Tracebacks are observed when the trustpoint is removed abnormally and the **no sccp** and **sccp** commands are entered.

  Conditions: This symptom is observed when the **no sccp** and **sccp** commands are entered after the trustpoint has been removed abnormally.

  Workaround: There is no workaround.

- CSCsy41063

  Symptoms: A Cisco router may display the following error message:

  ```
  %SYS-2-BADBUFFER: Attempt to use Mismatch sized buffer as scattered src, ptr=
  83BB71E0, pool= 83A4F670 -Process= "<interrupt level>", ipl= 2, -Traceback= 0x808DA290
  0x80087808 0x801BAF9C 0x800E5954 0x800E73F0 0x80369148 0x8008590C 0x8008590C
  0x80369208 0x8036D334 0x81957024 0x8036B57C 0x80375294
  ```

  Conditions: This symptom is observed with Q-in-Q configuration on the device.

  Workaround: There is no workaround.

- CSCsy49927

  Symptoms: IOSD restart seen with crest proc that fetches the tcl shell for execution.

  Conditions: This symptom is observed with a crest proc that helps in configuring a scale configuration.

  Workaround: There is no workaround.

- CSCsy54137

  Symptoms: Some calls are shown as active after a WAN link outage between the gateway and Call Manager.

  Conditions: The symptom is observed if a WAN outage happens when more than 40 calls are in progress. Some random calls are then shown to be as active when using the command **show call active voice compact** with Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCsy61321

  Symptoms: Accounting requests sent to the TAC server do not fail over to the second server.

  Conditions: This symptom is observed when two TACACS servers are configured, the first without TACACS, the second with TACACS, and authentication is configured as "none."

Workaround: Use a single working server, or ensure that the first group uses a valid server.

- CSCsy70524

  Symptoms: A router crashes upon deleting range PVCs with PPPoE sessions and with bandwidth configured through DBS.

  Conditions: The symptom is observed when deleting the range PVCs with PPPoE sessions.

  Workaround: There is no workaround.

- CSCsy74023

  Symptoms: A slow memory leak occurs, mainly in the 72 bytes, 80 bytes, and possibly 192 bytes memory regions blocks.

  Conditions: This symptom is observed with a large number of IPSec peers (>100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

  Workaround: There is no workaround.

- CSCsy89795

  Symptoms: A Cisco ASR 1000 series router may fail, and the console will display an error message similar to the following:

  ```
  "A critical process ppc_linux_iosd_image has failed (rc 139)".
  ```

  Conditions: This symptom is observed when using the **clear counters** command after removing a crypto map from an interface.

  Workaround: Wait a minute or two after removing a crypto map from an interface before entering the **clear counters** command.

- CSCsz18573

  Symptoms: A number of problems are found in the early version of the NEMO mobile router:

  - MR tunnel will flap with NEMO explicit prefix configured.
  - Roaming can be slow or fail installing routes.
  - MR routes appear as static as opposed to mobile.
  - Configuring the home address on a loopback is required.
  - ND operates on the MIP tunnel.
  - Ten seconds latency appears on MR at tunnel setup and on HA at roaming.

  Conditions: These symptoms occur when running Cisco IOS Release 12.4(22)T1 and Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCsz29542

  Symptoms: In the current implementation, “cwmp agent” identifies the WAN uplink if it has “cwmp wan default” configured on it. The WAN uplink interface differs, based on the router type used as a CPE. For the Cisco 871 router, WAN interface is FastEthernet 4 and for a Cisco 2811 router it is Fast Ethernet 0/0. This creates a problem in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

  Conditions: The symptom is observed in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

  Workaround: There is no workaround.

- CSCsz39167

  Symptoms: If a tunnel is configured over the 880-3G cellular interface, traffic forwarding stops when the packet size is greater than the tunnel MTU.

  Conditions: The symptom is observed when a tunnel is configured over a cellular interface and running Cisco IOS Release 12.4(24)T.

  Workaround: Disable “ip cef.”

- CSCsz68709

  Symptoms: A console may lock when using the **scripting tcl init** *init-url* command.

  Conditions: This symptom is observed when using the **scripting tcl init** *init-url* command where the *init- url* is invalid or inaccessible, then entering the **tclsh** command and appending a file name.

  Workaround: Ensure that the *init-url* argument used in the **scripting tcl init** command is valid and accessible.

  Alternate workaround: Enter the **tclquit** command to end the Tcl shell and return to privileged EXEC mode, then enter the **tclsh** command to enable the Tcl shell again.

- CSCsz71787

  Symptoms: A router crashes when it is configured with DLSw.

  Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

  Cisco IOS devices that are configured for DLSw with the **dlsw local- peer** command automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id** *IP- address* command listens for IP protocol 91 packets and UDP port 2067.

  Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

  ```
  dlsw remote-peer 0 fst <ip-address>
  ```

  It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

  Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

  As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

  ```
  dlsw remote-peer 0 fst <ip-address>
  ```

  If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature.
access-list 111 deny udp host 192.168.100.1 any eq 2067 access-list 111 deny 91 host
192.168.100.1 any
!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.
access-list 111 permit udp any any eq 2067 access-list 111 permit 91 any any
!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.
class-map match-all drop-DLSw-class match access-group 111
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-DLSw-traffic class drop-DLSw-class drop
!--- Apply the Policy-Map to the Control-Plane of the
!--- device.
control-plane service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic class drop-DLSw-class police 32000 1500 1500
conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at:

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

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

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
!--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067 access-list 150
deny 91 any INFRASTRUCTURE_ADDRESSES MASK
!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations.
!--- Permit all other traffic to transit the device.
access-list 150 permit ip any any
interface serial 2/0 ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

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

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in a customer environment.

- CSCsz72142

  Symptoms: Memory corruption may occur.

  Conditions: This symptom may be observed after issuing the **clear ip bgp soft** command on a BGP session which includes a connector attribute.

  Workaround: There is no workaround.

  Further Problem Description: This symptom was found by automated analysis tools, but has not been seen to have any real-world impact.

- CSCsz83570

  Symptoms: SSH sessions disconnect during large data exchanges, such as large logs with pagers.

  Conditions: The symptom is observed when large amounts of data are exchanged between both ends: client and server (i.e.: the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

  Workaround: Use 3DES for encryption.

- CSCsz89093

  Symptoms: A Cisco 2800 router may drop multicast packets.

  Conditions: This symptom is observed when stream sources are connected to an NM-16ESW switch module.

  Workaround: Disable IGMP snooping.

Further Problem Description: Packet loss can be seen with as little as 1 stream consisting of 1500 byte packets @ >= 1470pps. Packet loss can be viewed as follows:

```
zmrd# zmrd#sh int Fa1/1 stat
FastEthernet1/1 Switching path Pkts In Chars In Pkts Out Chars Out Processor 100000
150000000 53 4028 Route cache 0 0 0 0 Total 100000 150000000 53 4028 <--- 100,000 pkts
received zmrd# zmrd#sh int Vlan200 stat
Vlan200 Switching path Pkts In Chars In Pkts Out Chars Out Processor 0 0 0 0 Route
cache 99997 149595512 0 0 Total 99997 149595512 0 0 <--- 3 pkts dropped zmrd#
```

- CSCsz89826

  Symptoms: The router starts reloading while testing the OAM management functionality over ATM using the encapsulation aal5mux ppp which is done after the encapsulation aal5snap.

  Conditions: This symptom is observed after configuring “oam-pvc manage 9" under OAM feature.

  Workaround: There is no workaround.

- CSCsz93306

  Symptoms: Cisco IOS SCEP replies with the configured hash and encryption algorithm (the default is md5/des), instead of replying with the hash and encryption algorithms used by the client.

  Conditions: This symptom is observed under normal conditions.

  Workaround: Since the main concern is that less secure algorithms may be used in the reply than the request, administrators can match the algorithms configured for the clients in the Cisco IOS CA. That being said, you can only set the hash algorithm, and not the encryption algorithm. For that there is no workaround.

- CSCta08194

  Symptoms: A router may crash.

  Conditions: This symptom is observed when reprovisioning an AToM tunnel with AAL5 encapsulation.

  Workaround: There is no workaround.

  Further Problem Description: A complex sequence of events with specific timing characteristics is required to hit this crash.

- CSCta09049

  Symptoms: A memory leak chunk in alloc-proc “encrypt proc” with the name “Packet Header” is observed.

  Condition: This symptom is observed with software crypto enabled. The same configuration and traffic running with onboard-VPN does not have the leak.

  Workaround: Configure “no ip cef optimize neighbor resolution.”

- CSCta11223

  Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

  Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

  Workaround: There is no known workaround.

- CSCta14505

  Symptoms: No source group (SG) entry forms in the network for PIM sparse-mode groups. This leads to traffic failures.

Conditions: This symptom is observed when PIM-SM is configured in the network and traffic is sent for PIM-SM groups.

Workaround: Shut down the upstream interface, remove the IP address, configure it again, then perform a **no shutdown** on the interface.

- CSCta16724

  Symptoms: Users with level 15 privilege and a “view” cannot do a Secure Copy (SCP).

  Conditions: The symptom is observed when a user with a “view” attempts to do an SCP.

  Workaround: Remove view.

- CSCta17774

  Symptoms: An abnormal/high interarrival jitter time is reported in RTCP from a Cisco AS54xx when Nextport DSPs are used.

  Conditions: This symptom is observed under the following conditions:

  – Nextport DSPs are used on a Cisco AS54xx.

  – RTCP is used to measure interarrival jitter values.

  Workaround: There is no workaround.

- CSCta19962

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

- CSCta20590

  Symptoms: A group member (GM) pseudotime may desynchronize after re- registering or at initial registration.

  Conditions: This symptom is observed when GETVPN with time-based anti-replay (TBAR) is enabled.

  Workaround: Disable TBAR or use a very large window (> 30 seconds).

  Further Problem Description: After establishing phase I, the GM is supposed to obtain the KEK and TEKs. If a packet drop occurs (usually, this message is fragmented across multiple frames], then the router is not able to reassemble the packet. IKE will later resend this message, but if the pseudotime has not been recalculated the symptom will reoccur.

- CSCta21492

  Symptoms: PPP callback may fail.

  Conditions: This symptom is observed when MLP is configured under the dialer.

  Workaround: There is no workaround.

- CSCta22767

  Symptoms: A Cisco router may crash when unconfiguring class-map.

  Condition: This symptom is observed in a Cisco router using Cisco IOS Release 15.0M.

  Workaround: There is no workaround.

- CSCta30439

  Symptoms: Cisco routers with NPE-G1 and NPE-G2 may crash.

  Conditions: This symptom is observed when MLP is configured on CJ-PA and OIR is performed.

  Workaround: There is no workaround.

- CSCta32825

  Symptoms: A Cisco router may crash with a bus error after configuring a class-map or modifying a class-map.

  Conditions: This symptom is observed when using the **class-map** command in global configuration mode and the **match** command in class-map configuration mode. For example, entering the following commands may result in a crash:

```
*router(config)#class-map match-any PRIO
*router(config-cmap)#match dscp cs4
*router(config-cmap)#match dscp cs4 af41
*router(config-cmap)#match dscp cs4 af41 af42
*router(config-cmap)#match dscp cs4 af41 af42 af43
*router(config-cmap)#match dscp cs4 af41 af42 af43 ef
*router(config-cmap)#match dscp cs4 af41 af42 af43 ef cs5 <---device crashes here
```

  Workaround: Configure QoS changes when no traffic is passing through the router. This has only been seen while traffic is trying to match against the policy while it is being updated.

- CSCta37063

  Symptoms: NAT fails to translate H323 payload information.

  Conditions: This symptom occurs when NetMeeting is dialing from outside NAT to inside NAT.

  Workaround: Initiate NetMeeting again. Note that once this NAT entry is cleared or has timed-out, the issue will reappear.

- CSCta39339

  Symptoms: Traffic loss occurs on a Cisco ES20 line card when configuring IPv4 IP address on the SVI interface.

  Conditions: This symptom is observed when an xconnect configuration exists.

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

- CSCta49840

  Symptoms: GGSN may encounter a fatal error in VPDN/L2TP configurations.

  Conditions: The symptom is observed in rare race conditions when physical connectivity on the interface to LNS is lost while there are active sessions and traffic.

  Workaround: There is no workaround.

- CSCta50110

  Symptoms: A GM does not register.

  Conditions: This symptom is observed when a crypto map is attached to a tunnel interface only.

  Workaround: Apply the crypto map to the tunnel source physical interface as well.

- CSCta56762

  Symptoms: A Cisco router acting as an IP SLA Responder may leak memory in the chunk manager.

  Conditions: The symptom is seen when the router is responding to VoIP RTP probes.

Workaround: Stop the probes.

- CSCta59045

  Symptoms: If 32k dual-stack sessions are configured on a PTA device such as a Cisco ASR 1000, the router may crash when the sessions are brought down.

  Conditions: This symptom is observed when both the PPPoE client and the PTA are Cisco ASR 1000 routers. The client crashes when the **test pppoe** command is entered while trying to bring up 16K dual-stack sessions on the PTA device. This symptom is more likely to be observed when the preferred lifetime and valid lifetime of the assigned prefix are configured to be equal. The crash may occur even if the lifetimes are not equal, but it is less likely.

  Workaround: Do not configure the valid and preferred lifetimes of the prefix equally. This will decrease the probability of this crash, but does not ensure against it.

- CSCta66499

  Symptoms: The Cisco IOS MGCP gateway may experience a software-forced reload.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T4 or a later release when reenabling MGCP with version 1.0 after testing fgdos calls with MGCP version 0.1.

  Workaround: There is no workaround.

- CSCta69213

  Symptoms: A Cisco router configured for NHRP may crash due to a bus error.

  Conditions: This symptom is observed on a Cisco router configured for NHRP and DMVPN.

  Workaround: There is no workaround.

- CSCta75923

  Symptoms: One-way voice may occur after a transfer through a CMM transcoder if the stream goes through an RTP-aware firewall such as an ASA. The transcoder in some transfer situations will reuse a previous SSRC, which causes a security violation.

  Conditions: In a situation where there are 3 SSRCs in a single transfer, the outgoing stream from the transcoder will reuse the first SSRC in place of the third SSRC. This is against the RTP RFC, and some firewalls may drop the packet. Some gateways and endpoints may also not correctly process the packets, depending on the strictness of the RFC implemented.

  Workaround: It was found that some endpoints, like the Cisco Unified IP Phone 7960, activated a transfer with only 2 SSRC changes. It was also found that a Cisco Unified IP Phone 7941 with firmware 8-3-2 had the problem, but the latest 8-4-X image did not. Some endpoints, such as an autoattendant, do not have the ability to change this behavior. The only other workaround is to use a different type of transcoder than the ACT CMM.

- CSCta76251

  Symptoms: VPLS AD may not work after BGP has converged.

  Conditions: This symptom is observed when all of the PE routers are reloaded at the same time.

  Workaround: Configure MPLS IP by entering the **mpls ip** command on one of the tunnel interfaces.

- CSCta77678

  Symptoms: RTP timestamp on the RFC 2833 event is modified. IP Phones are using RFC2833 to transport the DTMF signals, which causes problems with the Voicemail systems.

  Conditions: This symptom occurs when RTP header compression is enabled.

  Workaround: There is no workaround.

Further Problem Description: The problem disappears if cRTP is disabled. The issue is seen with Class-Based cRTP configured and also with other cRTP configuration types.

- CSCta77960

  Symptoms: TCP/TCB leak may occur on a Cisco voice gateway with an increasing number of sessions hung in CLOSEWAIT state.

  Conditions: This symptom occurs when the voice gateway is under normal use.

  Workaround: There is no workaround.

- CSCta92029

  Symptoms: MSDP SA is not received on an MSDP peer.

  Conditions: The symptom is observed when the first hop router is also the RP.

  Workaround: There is no workaround.

- CSCta93129

  Symptoms: An IP fragment may bypass virtual fragment reassembly (VFR) processing and create a VFR timeout, causing additional inner IP fragments to be dropped.

  Conditions: This symptom is observed when encrypted IPSEC packets are fragmented by the remote device (fragmentation after encryption) or somewhere in the network between the VPN termination routers. When the fragmented IPSEC packets are reassembled and decrypted, if the decrypted inner packet is also an IP fragment, the IP fragment bypasses VFR processing. The following conditions may cause this symptom to occur:

  1. VFR is enabled on the decryption side
  2. Fragmentation happens after encryption on the encrypting router, or in the path
  3. The inner IP packet is fragmented when received by the encrypting router.

  Workaround: Perform fragmentation before encryption on the sending side, and ensure that the proper IP MTU is used on the tunnel so that no fragmentation occurs after encryption.

  Further Problem Description: When IPSEC packets corresponding to the first inner IP fragment bypass VFP processing, the second inner IP fragment, even if too small to require IPSEC fragmentation, is decrypted and then sent for VFR processing. Due to the timeout created when the first IP fragment bypasses VFR processing, the second inner IP fragment is dropped.

- CSCta93703

  Symptoms: Packets may be sent out of order in an rfc4938 flow-controlled PPPoE session.

  Conditions: This symptom is observed when packets are queued due to insufficient credits and a traffic stream is active.

  Workaround: There is no workaround.

- CSCta94296

  Symptoms: Some voice commands go missing, the router freezes on bootup, or there may be a crash on bootup with the following message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address.
  ```

  This is possibly seen with “Unable to save the data for mode. Too many saves” being printed on bootup.

  Conditions: The symptom is observed when many global voice or CME commands are configured.

  Workaround: Remove some global voice or CME feature commands.

- CSCta95295

  Symptoms: A Cisco router terminates 100+ VPN tunnels when using CRL checking for the Phase 1 authentication.

  Conditions: If IKE gets stuck for any reason, it might cause IOMEM to be depleted completely, which could lead to a router crash.

  Workaround: Disable CRL checking or use pre-shared keys.

- CSCta95621

  Symptoms: Firewall performance degradation is seen for HTTP traffic.

  Conditions: The symptom is observed when configuring a Zone Based Firewall to match HTTP traffic.

  Workaround: There is no workaround.

- CSCta96479

  Symptoms: IPv6 PPPoX session setup rate is low, dropping to about 10 sessions per second.

  Conditions: This symptom is observed under the following conditions:

  1. High number of PPPOX sessions with ipv6 ACLs
  2. IPV6 ACEs use port number
  3. IPV6 ACEs use icmp fields

  Workaround: There is no workaround.

- CSCta98321

  Symptoms: AAA server for HTTP authentication cannot be configured on a Cisco 861 integrated services router (ISR).

  Conditions: This symptom is observed when configuring the AAA server for HTTP authentication on a Cisco 861 ISR.

  Workaround: There is no workaround.

- CSCta98976

  Symptoms: A Cisco IOS certificate server (CS) may crash during a CA certificate rollover.

  Conditions: This symptom is observed with similarly-named keys.

  Workaround: Rename similarly-named keys. For example, the keys named SubCA are a subset of the SSH keys named SubCA.server. Rename the SSH keys using the **ip ssh rsa keypair-name** command.

- CSCtb01505

  Symptoms: A Cisco router may crash when building an OSPF Network LSA.

  Conditions: This symptom is observed while unconfiguring ospf configurations.

  Workaround: There is no workaround.

- CSCtb05195

  Symptoms: Throughput degradation may occur on a Cisco integrated services router (ISR).

  Conditions: This symptom is observed in CEF/SVI TOE configurations when comparing specific performance metrics between baseline Cisco IOS Release 12.4 (23.5)pi10 and target Release 12.4(24.6)PI11n.

  Workaround: There is no workaround.

- CSCtb09167

  Symptoms: The following issues can be observed with the PI11 image with a simple setup on both NPE-G1 and NPE-G2:

  1. There is a ~50% degradation on forwarding performance (with service reflect) on NPE-G1 when compared with Cisco IOS Release 12.4T.
  2. When the traffic rate goes higher than the router's capacity, traffic will not recover afterwards, even if the traffic is reduced back to a very low rate.

  Conditions: The symptom is specific to the service reflect feature.

  Workaround: There is no workaround.

- CSCtb11373

  Symptoms: Enabling IPv6 inspection debugs may lead to a Cisco router crash when traffic is passing through the device.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(21) with the following debug commands:

  - **debug ipv6 inspect tcp**
  - **debug ipv6 inspect detailed**
  - **debug ipv6 inspect events**

  Workaround: Do not use the above IPv6 inspection debug commands.

- CSCtb13015

  Symptoms: Virtual access on the LNS fails to obtain the template IP address.

  Conditions: This symptom is observed when

  1. a VPN profile template cisco-avpair is configured as follows:

```
template:ip-addr=10.10.10.10 255.255.255.255
```

  2. A PPPoE session is established from the client to the LNS. The call comes up, but the virtual access on the LNS fails to obtain the template IP address "10.10.10.10."

  Workaround: There is no workaround.

- CSCtb13421

  Symptoms: The GM may not register on a Cisco ASR 1000 series router.

  Conditions: This symptom is observed when a crypto map with local-address configured is applied on multiple interfaces, and one of these interfaces is then shut.

  Workaround: Disable local-address for the crypto map.

- CSCtb13472

  Symptoms: An LDP session flap occurs between PE and P routers. A large number of LDP sessions going down may cause all LDP sessions within the routing context to go down temporarily, and then come back up (i.e.: flap).

  Conditions: This symptom is observed with 100 LDP-targeted sessions between the PEs. When the targeted sessions flap, the link session between PE and P routers also flaps. The symptom is not restricted to just targeted sessions flapping. Any large number of LDP sessions flapping within a routing context could cause all LDP sessions within the routing context to flap. In this example, all the LDP sessions are within the default (non-VRF) routing context.

  Workaround: There is no workaround.

- CSCtb17152

  Symptoms: A large packet drop may occur when FRF.12 is enabled.

  Conditions: This symptom is observed when FRF.12 is enabled.

  Workaround: There is no workaround.

- CSCtb17856

  Symptoms: H323 calls may intermittently fail with Cause Code 41. After several days and depending on traffic, calls may start failing with Cause Code 47.

  Conditions: This symptom is observed when there is a race condition in setting up an H245 session between H323 peers and two separate H245 sessions are opened simultaneously.

  Workaround: There is no workaround for Cause Code 41. For Cause Code 47, reload the router to temporarily alleviate the symptoms.

- CSCtb21428

  Symptoms: An interface does not attempt to restart after restart-delay is configured.

  Conditions: When the serial interface is down for some reason and you have configured restart-delay on the serial interface, the interface should try to restart.

  Workaround: There is no workaround.

- CSCtb22889

  Symptoms: SIP(TLS--SIP CUBE) may experience up to 2-3 seconds of post-dial delay due to TLS processing. Processing delays of 1000 ms, 600ms, and 200ms are seen between the gateway TLS responses.

  Conditions: This symptom is observed with a TLS connection to another gateway.

  Workaround: Use the **sip-ua timers connection aging tls** *time* command to increase the time in the gateway TLS aging timer and therefore lower the frequency of the problem with the aging TLS timer.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

  1. Use the command **debug condition username**
  2. Bring up a VPDN session
  3. Clear the VPDN tunnel on LAC
  4. Remove the conditional debug.

  Workaround: There is no workaround.

- CSCtb26396

  Symptoms: HTTPS connections suddenly fail with the following error:

  ```
  //-1//HTTPC:/httpc_ssl_connect: EXIT err = -3, hs_try_count=1
  //394376//HTTPC:/httpc_process_ssl_connect_retry_timeout: SSL socket_connect failed
  fd(0)
  ```

  Conditions: The symptom is observed with CVP Standalone deployment running with HTTPS and with Cisco IOS Release 12.4(22)T1 or Release 12.4(24)T1.

  Workaround: Reload the gateway.

- CSCtb27747

  Symptoms: An active RP module may crash or the entire system may reload while the user is scrolling through the output of the **sh xconnect rib detail** command.

  Conditions: This symptom is observed when remote PEs in the VPLS mesh are reloading and some are in the process of booting up. The user has to pause and then continue the output of the **sh xconnect rib detail** command while the remote PEs are being added or deleted.

  Workaround: Do not enter the **sh xconnect rib detail** command while remote PEs are being added or deleted.

- CSCtb34358

  Symptoms: Tunnel sources get mixed up when tunnel interfaces are configured with serial subinterfaces as sources and the router is reloaded.

  Conditions: The symptom occurs only after a reload or when a saved configuration is applied to the running configuration.

  Workaround: There is no workaround.

- CSCtb34814

  Symptoms: The following error message is reported just before a crash:

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

  There may not be any tracebacks given for the crash.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCtb36521

  Symptoms: A Cisco Catalyst 6500 may stop processing IKE traffic, which results in IPSec tunnels not working. Under extreme circumstances, system IO memory might become completely depleted, at which point all traffic processing will stop.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 with a VPN-SPA module running a Cisco IOS SXH image when PKI infrastructure is used to authenticate IKE peers. The certificate in use must contain a CDP that uses HTTP protocol to retrieve the CRL. Revocation-check must be configured to fetch the CRL using the **revocation-check** *crl* or **revocation-check** *crl none* command.

  Workaround: Disable CRL validation by using the **revocation- check** *none* command instead of the **revocation-check** *crl* or **revocation-check** *crl none* commands in the trustpoint being used. Note that disabling CRL validation poses a possible security risk.

  Alternate Workaround: Create a certificate map tied to the trustpoint in use to override the CDP using a URL which specifies the IP address of the CDP server instead of a name. For example, if the router1 certificate tied to cdp_override trustpoint contains a CDP URL such as:

  ```
  http://ca_server.yourdomain.com:80/crl.txt
  ```

  replace it with the ca_server.yourdomain.com IP address by using:

  ```
  crypto pki trustpoint cdp_override match certificate cert_map_1 override cdp url
  http://XXX.xxx.x.x:xx/crl.txt

  crypto pki certificate map cert_map_1 1 subject-name co router1
  ```

- CSCtb36637

  Symptoms: The registering flag gets set on Mroute entry. Register-Stop is not received from the RP.

Conditions: The symptom is observed when sending the data packets before the RP address interface comes up in RP. It is observed on a Cisco 7200 series router that is running the 12.4(24.6)PI11r image.

Workaround: There is no workaround.

- CSCtb37756

  Symptoms: A Cisco router acting as NAS rejects an IPCP request from the client.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24.6) under the following conditions:

  1. Clients connect over BRI lines and legacy dialer is configured on both the clients and NAS
  2. Multilink is configured on the client and NAS [Dialer Hunt group scenarios]
  3. Radius authentication is used and, during authentication, per-user attributes are downloaded.

  Workaround: Configure the RADIUS server so that per-user attributes are not sent in Access-Accept or Access-Challenges (EAP case). Since this is Legacy Dialer and BRI, multiple user sessions are not really seen and hence the required attributes can be configured locally on router.

- CSCtb39345

  Symptoms: Session timeout does not occur within the time configured in the session-timeout value on a per-user profile.

  Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCtb40985

  Symptoms: The memory occupied by the Cisco IP SLAs Sync Pro may gradually increase.

  Conditions: This symptom is observed on a Cisco Supervisor Engine 720 (sup720- 3B) with a Cisco IOS Release 12.2(33)SXI1 image when ICMP path jitter operation is configured on the router with an invalid source address.

  Workaround: Configure the SLA operation with the correct source address.

- CSCtb43009

  Symptoms: A Cisco 3845 router crashes when key server is removed from the list.

  Conditions: The symptom is observed with the following configuration on a GM router:

  ```
  conf t crypto gdoi group GetvpnScale1 identity number 1111 no server address ipv4
  10.10.1.4
  ```

  When a unicast rekey is received, the router crashes.

  Workaround: There is no workaround.

- CSCtb43293

  Symptoms: ACL functionality may break on a Cisco 10000 series router after redundancy switchover.

  Conditions: This symptom is observed after a redundancy switchover on a PPPoX session with ACL applied.

  Workaround: There is no workaround.

- CSCtb44031

  Symptoms: An LDP session goes down and does not re-establish.

Conditions: This symptom is observed when the password is removed from the LDP session on both peers with the **no mpls neigh** *ip- address* **password** *password* command.

Workaround: There is no workaround.

- CSCtb44167

  Symptoms: A Cisco router may reload when running EAP- FAST authentication with RADIUS Accounting.

  Conditions: This symptom is observed on a Cisco 1841 integrated services router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCtb45057

  Symptoms: A fax through a Cisco IOS gateway configured for Fax Relay to a Cisco fax server fails.

  Conditions: When there is an incoming fax call on the Cisco IOS gateway that is configured for Fax Relay, the fax call setup between the gateway and the Cisco fax server fails. This symptom occurs when the Cisco fax server is configured to receive calls on an H.323 call control module.

  Workaround: There is no workaround. Configure SIP between the Cisco IOS gateway and the Cisco fax server if that is an acceptable workaround.

- CSCtb45718

  Symptoms: A Cisco router may crash with traceback leading to checkheap.

  Conditions: This symptom is observed when endpoint agnostic port allocation has been enabled using the **ip nat service enable-sym-port** command.

  Workaround: Disable the endpoint agnostic port allocation using the **no ip nat service enable-sym-port** command.

  Further Problem Description: Under certain conditions, the symmetric port database is not in sync with the port list, resulting in the reuse of port ranges that had been free.

- CSCtb46556

  Symptoms: With a CJPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2, the NPE-G2 sometimes crashes when executing the command **clear int range multilink 1 10** and the NPE-G1 gives spurious access for the same command.

  Conditions: The symptoms are observed with a CJPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2 and when 14 multilinks are configured with two members each. Pagents are sending bi-directional traffic.

  Workaround: Do not perform commands across all interfaces using interface range. Perform the commands one-by-one, manually.

- CSCtb48397

  Symptoms: A Cisco ISR router may experience performance degradation due to corrupted TCP headers.

  Conditions: This symptom is observed on a Cisco ISR router with Cisco IOS Release 12.4 or Release 12.4T running interface-based TCP header compression on any data link. Corrupted TCP headers may occur when all of the following are true:

  1. Frame-Relay, PPP, or HDLC is configured with “ip tcp header-compression”
  2. The queueing mechanism is fair-queue (either interface-based or in map- class frame-relay)
  3. >1 TCP sessions are traversing the compressing mechanism
  4. The packets are in the hardware (CEF) switching path.

Workarounds:

1. Do not configure an interface to carry compressed TCP/IP headers using the **frame-relay ip tcp header-compression** command.
2. Disable hardware switching for all interfaces on the Cisco ISR using the **no ip route-cache** command.
3. Do not use any form of fair-queue on interfaces configured with the **frame-relay ip tcp header-compression** command. To remove fair-queue, use the **no fair-queue** command in policy-map class configuration mode.

Further Problem Description: With exactly two MS Remote Desktop Protocol TCP sessions, when the UUT's serial transmit-ring (or frame-relay shaper Bc) congests and the fair-queue invokes, the compressed header from the second- established TCP flow is erroneously written into headers of some packets from the first-established TCP flow, resulting in post-decompression frames erroneously added to the first-established TCP flow and erroneously removed from the second-established TCP flow, thereby causing a performance degradation.

- CSCtb48984

  Symptoms: SSLVPN Login Page is not being properly displayed on mobile devices. Also, there is no support for iPhone and iPod safari browsers.

  Conditions: The symptom is observed on an access page using Windows Mobile, or on an iPhone or iPod.

  Workaround: Page will be displayed but quality will be poor.

- CSCtb51922

  Symptoms: Chunk leak of list element when a host-address under a PfR API provider is configured or unconfigured.

  Conditions: This symptom is observed when the following occur:

  1. PfR MC is configured
  2. API provider with a host address is configured
  3. Host address is unconfigured, or the MC process is shut/no shut.

  Workaround: There is no workaround.

- CSCtb51993

  Symptoms: A router crashes upon bringing up PPPoE sessions.

  Conditions: The symptom is observed when AAA proposes a pool name but the pool is not defined on the NAS as well as the radius.

  Workaround: Define the pool on the NAS or as a dynamic pool on the radius.

- CSCtb52200

  Symptoms: A router may crash when configuring 3-level policies with strict priorities on each level.

  Conditions: This symptom is observed when:

  - the bandwidth value configured for the interface is very low
  - a class in the parent policy has a bandwidth of less than 1kbps
  - a child policy is added with priority or Bandwidth Remaining Percentage (BRP).

  Workaround: When attaching a child policy with priority or BRP, ensure that the parent class bandwidth is greater than 1kbps.

- CSCtb54422

  Symptoms: An MFR bundle moves from SW to HW mode and flaps after reload.

  Conditions: This symptom is observed on a Cisco 7200 router when an MFR is configured on CJ-PA, then one member is added from MCTE1 and the following commands are entered: **wr mem** and **reload**.

  Workaround: Create a new MFR after reload and add members to it.

- CSCtb56567

  Symptoms: A Cisco voice gateway experiences a memory leak error on CCSIP SPI CONTROL process, which may lead the router to crash every 4-5 days.

  Conditions: This symptom is observed when a router is configured with sip- ua using the **mwi-server** command with transport set to *tcp*, but the server specified is not set up to receive sip and thus replies with tcp resets. This can be caused by misconfigured sip mwi.

  Workaround: Reload the device regularly to free the memory.

- CSCtb57180

  Symptoms: A router may crash with a software-forced crash.

  Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

  Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

  The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

  Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255 Router(config)# access-list 1 permit host 172.16.1.2 Router(config)# line vty 0 4 Router(config-line)# access-class 1 in

  For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

  Router(config)# line 1 <x> Router(config-line)# access-class 1 in

  Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

  Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

  1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
  2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.
  3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.
  4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.
  5. Avoid issuing the **show users** command repetitively in a short period of time.

  Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- CSCtb57237

  Symptoms: After a call is resumed from hold, the gateway sends a G.729 codec although a G.711 was negotiated in the H.245 messages.

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

  Workaround: There is no workaround.

- CSCtb58160

  Symptoms: A router crashes upon bootup.

  Conditions: The symptom is observed when reloading a router with the NAM module configured.

  Workaround: There is no workaround.

- CSCtb58724

  Symptoms: The symptoms are:

  1. Incomplete rekey/ANN seqnum checking. This may cause inaccuracy in detecting seqnum errors in Co-operative key server (COOP KS) split/merge corner cases.
  2. After using the command **clear cry gdoi** on the GM, the GM may not register successfully due to a PST difference between the key server and the GM.

  Conditions: The symptom is observed in corner cases of COOP KS split/merge scenarios.

  Workaround: There is no workaround.

- CSCtb60603

  Symptoms: The router crashes and resets when you try to execute the following command: **show run | format** *x* (where x = any keyword).

  Conditions: The symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(24)T. The router needs to have a general route-map configured.

  Workaround: Do not execute **show run | format** *x* if there is a general route-map configured in the router.

- CSCtb62177

  Symptoms: Downspeeding stops based on Voice and 4-second silence.

  Conditions: This symptom is observed on a Cisco AS5400.

  Workaround: An image with a partial short-term solution was released on 08-09-2009. With this image, module changes are done, and the CLI is implemented to drop 4-second silence events and voice packets.

- CSCtb64686

  Symptoms: When a VC bundle is configured and traffic is passed at a high rate, the output packet counters may show an incorrect and very large value.

  Conditions: This symptom is observed only in Frame Relay PVC counters. The **show interface** command displays proper output.

  Workaround: There is no workaround.

- CSCtb65151

  Symptoms: A device might crash with a bus error and the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

Conditions: The symptom is observed on a device that is running Cisco IOS Release 12.4(24)T1. Other releases may be affected (those running with the Common Classification Engine). The condition seems to be temporary and after a while it goes away.

Workaround: There is no workaround.

- CSCtb66295

  Symptoms: No ip connectivity exists due to erroneous ARP tables.

  Conditions: This symptom is observed when NAT and HSRP are configured on the same interface.

  Workaround: There is no workaround.

- CSCtb66925

  Symptoms: A router may crash during a port scan to TCP port 53.

  Conditions: DNS functionality must be configured on the device.

  This crash has been observed only in Cisco IOS Release 12.4(24)T, Release 12.4(24)T1, and Release 12.4(22)T. It is a timing condition on processing DNS TCP traffic.

  Workaround: Create an ACL to deny traffic to the device on TCP port 53:

  The following mitigations have been identified for this Cisco bug ID, which may help protect an infrastructure until an upgrade to a fixed version of Cisco IOS software can be scheduled:

  * Infrastructure Access Control Lists (iACLs)

  Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access list, which will protect all devices with IP addresses in the infrastructure IP address range:

  ```
  !---
  !--- Feature: DNS over TCP
  !---
  access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
  !---
  !--- Deny DNS TCP traffic from all other sources destined
  !--- to infrastructure addresses.
  !---
  access-list 150 deny tcp any
      INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
  !---
  !--- Permit/deny all other Layer 3 and Layer 4 traffic in
  !--- accordance with existing security policies and
  !--- configurations. Permit all other traffic to transit the
  !--- device.
  ```

```
!---
access-list 150 permit ip any any
!---
!--- Apply access list to all interfaces (only one example
!--- shown).
!---
interface serial 2/0
 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

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

* Receive ACLs (rACLs)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the Cisco 12000, 12.0(24)S for the Cisco 7500, and 12.0(31)S for the Cisco 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor.

Receive ACLs are designed to protect only the device on which they are configured. On the Cisco 12000, 7500, and 10720, transit traffic is never affected by a Receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below refer only to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml

The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```
!---
!--- Permit DNS over TCP traffic from trusted hosts allowed to the RP.
!---
access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 53
!---
!--- Deny DNS over TCP traffic from all other sources to the RP.
!---
access-list 150 deny tcp any any eq 53
!--- Permit all other traffic to the RP according
!--- to security policy and configurations.
access-list 150 permit ip any any
!--- Apply this access list to the 'receive' path.
```

```
ip receive access-list 150
```

* Control Plane Policing

Control Plane Policing (CoPP) can be used to block the affected features TCP traffic access to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

The CoPP example below should be included as part of the deployed CoPP that will protect all devices with IP addresses in the infrastructure IP address range.

```
!---
!--- Feature: DNS over TCP
!---
access-list 150 deny tcp TRUSTED_HOSTS WILDCARD any eq 53
!---
!--- Permit DNS over TCP traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so
!--- that it will be policed and dropped by the CoPP feature.
!---
access-list 150 permit tcp any any eq 53
!---
!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and
!--- Layer 4 traffic in accordance with existing security policy
!--- configurations for traffic that is authorized to be sent
!--- and to infrastructure devices.
!--- Create a class map for traffic to be policed by
!--- the CoPP feature.
!---
class-map match-all drop-tcp-class
 match access-group 150
!---
!--- Create a policy map that will be applied to the
!--- control plane of the device.
!---
policy-map drop-tcp-traffic
 class drop-tcp-class
  drop
```

```
!---
!--- Apply the policy map to the
!--- control plane of the device.
!---
control-plane
 service-policy input drop-tcp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that the policy-map syntax is different in the 12.2S and 12.0S Cisco IOS trains:

```
policy-map drop-tcp-traffic
 class drop-tcp-class
  police 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature can be found in the documents "Control Plane Policing Implementation Best Practices" and "Cisco IOS Software Releases 12.2 S - Control Plane Policing" at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

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

- CSCtb66963

  Symptoms: A SIP call from a call-forwarded phone to a Cisco IOS VoIP gateway is rejected when INVITE contains a comma in the Diversion Header.

  Conditions: Example of an inbound SIP invite that contains a Diversion field such as this:

```
---- Received: INVITE sip:15551111111@10.1.134.116:5070 SIP/2.0 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 Remote-Party-ID:
<sip:5555555555@172.27.128.130>;party=calling;screen=yes;privacy=off From:
<sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879?
To: <sip:15551111111@10.1.134.116> Date: Sat, 29 Aug 2009 08:06:56 GMT Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Supported: timer,replaces Min-SE: 1800
User-Agent: Cisco-CCM5.1 Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK,
UPDATE, REFER, SUBSCRIBE, NOTIFY CSeq: 101 INVITE Contact:
<sip:5555555555@172.27.128.130:5070> Expires: 180 Allow-Events: presence
Session-Expires: 1800 Diversion: "Smith, John"
<sip:87007@172.27.128.130>;reason=unconditional;privacy=off;screen=no Max-Forwards: 7
Content-Type: application/sdp Content-Length: 214 ----
```

  The IOS gateway will respond back with the following:

```
---- Sent: SIP/2.0 400 Bad Request - "Malformed CC-Diversion/Diversion/CC-Redirect
Header" Reason: Q.850;cause=100 From:
<sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879
Content-Length: 0 To: <sip:15551111111@10.1.134.116>;tag=B8C0430-6C Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 CSeq: 101 INVITE ----
```

  Workaround: Modify the diverting name associated with the redirecting device so that it does not contain a comma.

- CSCtb67967

  Symptoms: PPP fails at LCP stage with VPDN dial-out calls.

Conditions: This symptom is observed in Cisco IOS Release 12.4T in a dial-out scenario.

Workaround: There is no workaround.

- CSCtb68229

  Symptoms: The box crashes within “cns config notify code”.

  Conditions: This symptom is observed in the corner case when someone removes “cns config notify diff” from the config while adding other CLIs to the running config by using the method “config replace”. The box can crash.

  Workaround: Do not remove “cns config notify diff” using “config replace”.

- CSCtb68539

  Symptoms: There may be problems with downloading large packages from remote server to local server.

  Conditions: The symptom is observed when the package size is approximately greater than 4KB.

  Workaround: Use small packages.

- CSCtb69063

  Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:

  ```
  config# username <name of 64 characters> priv <0-15> password 0 <password>
  ```

  Conditions: The symptom is observed if the user name is exactly 64 characters.

  Workaround: Configure a user name of less than 63 characters.

  Further Problem Description: When some configurations are added, modified, or deleted the **show configuration id detail** command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the “changed by user” field prints unwanted characters.

- CSCtb69796

  Symptoms: The tunnel stitching VC may go down, resulting in traffic loss.

  Conditions: This symptom is observed when the remote peer is changed with a different MTU, causing the tunnel stitching VC to go down. When the matching MTU is reconfigured, however, the tunnel stitching session does not come back up.

  Workaround: There is no workaround.

- CSCtb69859

  Symptoms: A Cisco router may crash with the following traceback:

  ```
  0x40A0D7E8 0x40A0C870 0x409D4DC4 0x4098E0AC 0x42655B74 0x40E3CE4C 0x40E3D634
  0x40E3DAB8 0x40974B78 0x40974B5C
  ```

  Conditions: This symptom is observed while configuring a DHCP address pool using the **ip dhcp pool** *TAL_DHCP_vrf_pool* command.

  Workaround: There is no workaround.

- CSCtb70102

  Symptoms: When SRST and STCAPP are configured and running on the same router, SCCCP-controlled analog phones may be unable to make an outgoing call.

  Conditions: This symptom is observed when, upon WAN link failure, the phones register to an SRST gateway.

Workaround: There is no workaround.

Further Problem Description: This symptom occurs due to STCAPP automatically adding a *station-id* parameter under the **voice-port** command in order to save DN information for registration to SRST.

- CSCtb71889

  Symptoms: DNS A-answer from IPv4 DNS server (which is supposed to be forwarded to IPv6 side as AAAA-answer) is dropped on NAT-PT routers.

  Conditions: The symptom is observed when DNS NAT-ALG is enabled.

  Workaround: There is no workaround.

- CSCtb72550

  Symptoms: Call Detail Record (CDR) files pushed via FTP are not created on the FTP server.

  Conditions: This symptom is observed when the **gw-accounting** *file* command is configured to point to an FTP server.

  Workaround: Push the CDR records locally to the flash instead of to an FTP URL.

- CSCtb72653

  Symptoms: The router crashes when unconfiguring a policymap from a virtual interface.

  Conditions: This issue is seen only when the interface is a virtual interface and the configuration is changed after the interface flaps.

  Workaround: There is no workaround.

- CSCtb72664

  Symptoms: 100% ingress packet drop (IQD) with depletion of free IO memory.

  Conditions: This symptom is observed in a Cisco 3945 [NM-1A-OC3-POM] <-> [NM-1A-OC3-POM] peer setup. In this or a similar scenario, stressing the OC3 module at the line rate (~84Mbps) with bi-directional traffic will cause this symptom along with depletion of free IO memory.

  Workaround: Do not stress the NM-1A-OC3-POM module at the line rate. Stopping or reducing the traffic rate should resolve the depletion of free IO memory.

- CSCtb75294

  Symptoms: A router crashes upon bringing up PPP sessions.

  Conditions: The symptom is observed if IP pools are configured.

  Workaround: There is no workaround.

- CSCtb76775

  Symptoms: A Cisco 3900 series router may experience a large IO memory leak.

  Conditions: This symptom is observed with IPSec and QoS on a Cisco NM-1A- T3/E3 network module with NME-IPS in promiscuous mode.

  Workaround: Run IPS in inline mode.

- CSCtb78266

  Symptoms: An incorrect NAS port ID is given when testing IDBless VLAN for PPPoE.

  Conditions: The symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 12.4(15)T10.

  Workaround: There is no workaround.

- CSCtb79211

  Symptoms: A Cisco AS5400XM may process switch all traffic through interfaces. Other platforms may be affected.

  Conditions: The symptom is observed if you are running Cisco IOS Release 12.4(20)T or later and the interface is configured for netflow with one of the following feature sets:

  - c5400-ik9s-mz
  - c5400-ik9su2-mz
  - c5400-jk9su2_ivs-mz

  Workaround: Disable netflow.

- CSCtb81833

  Symptoms: A Cisco router crashes due to a watchdog timeout during interface range port-channel.

  Conditions: This symptom is observed on a Cisco router after entering the **interface range port-channel** command with PPPoE configuration.

  Workaround: There is no workaround.

- CSCtb82256

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed when all of the following occur:

  - Cisco Unified CallManager XML configuration files are downloaded to the router while the router is processing the pri-group configurations
  - the **shutdown** and **no shutdown** commands are entered on the voice port and
  - the **no ccm-manager** command is entered.

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

- CSCtb83353

  Symptoms: After an RP switchover, the new active RP log shows many tracebacks and all sessions/tunnels are torn down.

  Conditions: The symptom is observed when LNS is configured with 16000 sessions/8000 tunnels (two sessions per tunnel); all sessions with Model D2 QoS. It is seen after an RP switchover.

  Workaround: There is no workaround.

- CSCtb83578

  Symptoms: A severe memory leak may occur on a Cisco CME router.

  Conditions: This symptom is observed on a Cisco CME router with the CCSIP- REGISTER process.

  Workaround: There is no workaround.

- CSCtb86203

  Symptoms: Degradation occurs when creating and bringing up 1k GRE/IPIP tunnels.

  Conditions: This symptom is observed only while scaling up to 1k tunnels.

  Workaround: There is no workaround.

- CSCtb86279

  Symptoms: Cisco IOS crashes at bootup.

  Conditions: The symptom is observed on a Cisco 1941 with 512MB of on-board memory.

Workaround: There is no workaround.

- CSCtb87856

  Symptoms: Router can crash with a `"%SYS-3-CPUHOG:"` when DMVPN is deployed.

  Conditions: The symptom is observed when the physical interface (tunnel source) of the router is shut, the routing neighbourship flaps, and memory consumption is increased to the point that there is no free memory left. This causes the router to crash.

  Workaround: There is no workaround.

- CSCtb88409

  Symptoms: A Cisco router may crash when configuring the object id in config-event-objlist subconfiguration mode.

  Conditions: This symptom is observed when entering the **cns config notify** command.

  Workaround: There is no workaround.

- CSCtb89424

  Symptoms: In rare instances, a Cisco router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

  ```
  hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC
  = 0x424ECCE4
  ```

  Conditions: This symptom is observed while using IP SLA.

  Workaround: There is no workaround.

- CSCtb89819

  Symptoms: A single ping packet with size that is greater than or equal to 1501 bytes will cause a router with an ATM interface to crash.

  Conditions: The symptom is observed only when NAT or “ip virtual-reassembly” is configured on an ATM interface.

  Workaround: There is no workaround.

- CSCtb90751

  Symptoms: FTP and HTTP protocols are not supported for the remote download of FPM packages.

  Conditions: The symptom is observed with the remote download of FPM packages.

  Workaround: Use TFTP, SCP, or HTTPS.

- CSCtb91412

  Symptoms: An IPv6 EIGRP session may go down if one of the IPv6 addresses configured on the interface is deleted.

  Conditions: This symptom is observed when more than one IPv6 address is configured on the interface, and one of the those addresses is then deleted.

  Workaround: There is no workaround.

- CSCtb91992

  Symptoms: A Cisco router may crash with chunk-related errors.

  Conditions: This symptom is observed on a router with IOS IPS configured after several hours of traffic.

  Workaround: There is no workaround, other than removing IOS IPS.

- CSCtb93855

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

- CSCtb95275

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

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

  Workaround: Explicitly configure user privilege in the user profile.

- CSCtb95801

  Symptoms: In certain network setups, every five days the router hangs and the following error message is seen:

  ```
  SYS-2-BADSHARE: Bad refcount in datagram_done
  ```

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCtb97176

  Symptoms: Router may reload unexpectedly shortly after boot up.

  Conditions: This symptom is observed when QoS is configured on a router running Cisco IOS Release 15.0M

  Workaround: Disable QoS by removing the service-policy statement applied to all interfaces.

  Alternate Workaround: Use a previous Cisco IOS release.

- CSCtb98080

  Symptoms: When you attempt to browse to a WebVPN portal you only see a blank page. The router does not send the browser a certificate and the portal login page is not displayed. The command **debug webvpn sdps** logs the following error message:

  ```
  WV-SDPS: Sev 4:sslvpn_tcp_read_notify(),line 1569:No to notify read: already queued[1]
  004549:
  ```

  Conditions: The symptom is observed when the SSLVPN process is waiting for an HTTP REQUEST from a client on the port configured using the **http-redirect** *<port no>* command but the process does not wake up. This can happen because of an unexpected IPC message to the SSLVPN process by another IOS process.

  Workaround: Remove **http-redirect** from the WebVPN gateway and reload the device.

- CSCtb98508

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

  Conditions: The symptom has been experienced on a Cisco 2851 router that is running Cisco IOS Release 12.4(20)T3 and when “callmonitor” is enabled.

  Workaround: There is no workaround.

- CSCtc03750

  Symptoms: The following error message can be seen on an SSO switchover:

  ```
  %RF-3-NOTIF_TID: Notification timer extended for the wrong client
  ```

  In addition, the secondary RP reloads continuously after an RP switchover.

  Conditions: The symptoms are observed when the router has been scaled with 2000 AToM, 1600 TE tunnels, 100 Ethernet over MPLS over GRE (EoMPLSoGRE) sessions, and 100,000 BGP routes.

  Workaround: There is no workaround.

- CSCtc04016

  Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW/CUBE may experience high CPU utilization, which causes additional calls through the router to fail.

  Conditions: This symptom is observed under rare conditions when SIP- associated processes on the Cisco IOS gateway (as seen when the **show process cpu** command is entered) cause extremely high CPU utilization, which causes further calls through the router to fail.

  Workaround: There is no workaround.

  Further Problem Description: This symptom occurs due to a SIP "491 Request Pending" and ACK loop between the gateway and a third-party device. This loop most often occurs in environments with a large number of SIP REFER transfers. To determine whether the loop is occurring, enter the **show sip statistics** command and look for the RequestPending value; a high and increasing output count could indicate the SIP loop.

- CSCtc04228

  Symptoms: The command **mgcp behavior g729-variants static-pt** is the default and will show up in the configuration. This causes a problem when you save the configuration and downgrade to an earlier Cisco IOS Release where this behavior is not present. There, the command will now be enabled when it was not previously.

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

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

- CSCtc04351

  Symptoms: The GM router might reload.

  Conditions: This symptom is observed if the following conditions are met:

  1. Many VRFs are configured on the same GM, each belonging to an individual GETVPN group.
  2. All the VRFs are triggered to register with the KS at the same time.
  3. While #2 is happening, the **clear crypto gdoi** command is entered on the GM.

  Workaround: There is no workaround.

- CSCtc05547

  Symptoms: Ping may fail on a Cisco 3845 integrated services router (ISR) or other low-end router where tunnel does not support turbo path.

  Conditions: This symptom is observed when L2VPN is configured over tunnel.

  Workaround: Do not configure L2VPN over tunnel.

- CSCtc06629

  Symptoms: A Cisco router may crash at crypto functions after upgrade to Cisco IOS Release 12.2(33r)XNC.

  Conditions: This symptom is observed on a Cisco ASR 1000 Series router after upgrading from Cisco IOS Release 12.2(33r)XNB to Release 12.2(33r) XNC.

  Workaround: There is no workaround.

- CSCtc09735

  Symptoms: CISCO-ICSUDSU-MIB does not report any values on SNMP query for a Cisco HWIC-1CE1T1-PRI card and its variants.

  Conditions: This symptom is observed when querying the CISCO-ISCUDSU-MIB by inserting a Cisco HWIC-2CE1T1-PRI card.

  Workaround: There is no workaround.

- CSCtc11521

  Symptoms: Invalid pointer value is displayed whenever NVRAM is accessed:

  ```
  "NV: Invalid Pointer value(460E460C) in private configuration structure"
  ```

  Conditions: This symptom is observed when upgrading NVRAM from an older version to a newer version.

  Workaround: Load a prior working image and backup all files in NVRAM, including the startup-config, to another device or tftp/ftp. Load the new image and enter the **erase/all nvram** command followed by the **write mem** command. NVRAM will now be restored. Copy the backup files back to NVRAM.

- CSCtc12312

  Symptoms: PKI might get stuck after 32678 failed CRL fetches, causing IKE to stop processing any further ISAKMP packets.

  Conditions: This symptom is observed in Cisco IOS Release 12.4.20T4 and Release 12.2(33)SXH5 when CRL checking is performed.

  Workaround: Do not perform CRL checking.

  Further Problem Description: Normally, this symptom could take years to manifest in a well-designed environment, but in extreme conditions it could occur within hours.

- CSCtc13085

  Symptoms: The keys used in the PI11 code for encrypting and decrypting FPM filters in eTCDF are dummy keys, used for internal testing. Those keys need to be replaced with actual keys for encrypting and decrypting filters.

  Conditions: The symptom is observed with the keys used in the PI11 code for encrypting and decrypting FPM.

  Workaround: There is no workaround.

- CSCtc13344

  Symptoms: Cisco Optimized Edge Routing (OER) experiences a fatal error and is disabled:

  ```
  %OER_MC-0-EMERG: Fatal OER error <> Traceback %OER_MC-5-NOTICE: System Disabled
  ```

  Conditions: This symptom is observed when configuring OER to learn the inside prefixes within a network by using the **inside bgp** command.

  Workaround: Disable prefix learning by using the **no inside bgp** command.

- CSCtc13664

  Symptoms: With an IPv6 Policy Based Routing (PBR) configuration, the route-map clause “set interface null0” may cause a router to crash.

  Conditions: The symptom is observed with IPv6 PBR. The trigger traffic is traceroute packets (ping packets will not cause the crash).

  Workaround: Configure “route-map” as [set interface loop0].

- CSCtc14156

  Symptoms: A router crashes while testing Redial Enhancement feature.

  Conditions: This symptom happens during the unconfiguration part of ISDN dialer profile.

  Workaround: Wait for a period of 30 seconds before starting the un- configuration.

- CSCtc16399

  Symptoms: NIOS watchdog timer times out.

  Conditions: This symptom is observed when an MC5727 modem is power-cycled.

  Workaround: Reload the router.

- CSCtc16589

  Symptoms: A Cisco router may crash when bringing up PPPoE sessions.

  Conditions: This symptom is observed when bringing up 1000 PPPoE sessions from two ends, one a client router and the other the equipment of a third-party vendor.

  Workaround: There is no workaround.

- CSCtc17162

  Symptoms: A Cisco router may crash due to a SegV exception.

  Conditions: This symptom is observed on a Cisco 2650XM router running Cisco IOS Release 12.4(15)T10 when VTI is configured inside the EzVPN.

  Workaround: Remove the VTI inside the EzVPN.

- CSCtc18562

  Symptoms: When Network Address Translation (NAT) of the outside source address is enabled, the static route to the local IP address is installed in the global RIB instead of the VRF RIB.

  Conditions: This symptom is observed when enabling NAT of the outside source address using the **ip nat outside source static** *global-ip local-ip* **vrf** *vrf name* **add-route extendable match-in-vrf** command.

  Workaround: Configure a static route within the VRF.

- CSCtc18841

  Symptoms: ARP entry of HSRP enters an “incomplete” state with an ip local- proxy-arp configuration even though the device receives an arp reply from the HSRP active router.

  Condition: This symptom is observed when “ip local-proxy-arp” is configured on the received arp reply of HSRP, and when the arp reply is received on the vlan interface.

  Workaround: Remove the ip local-proxy-arp configuration from the vlan interface, then shut/no shut the vlan interface.

- CSCtc21389

  Symptoms: IMA sub-interfaces do not come up.

Conditions: Occurs if the number of PVCs exceeds 255.

Workaround: Do not create more than 255 PVCs.

- CSCtc23003

  Symptoms: A Cisco device running Cisco IOS Software may unexpectedly reload with a STACKLOW message.

  Conditions: This symptom is observed when the **logging buffered xml** *xml-buffer-size* command is entered to enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer.

  Workaround: Disable the XML syslog buffer and return the size of the buffer to the default using the **no logging buffered xml** *xml-buffer-size* command.

- CSCtc23374

  Symptoms: A Cisco router may unexpectedly reload with the following message:

  ```
  %SYS-6-STACKLOW: Stack for process BGP Router running low, 0/9000
  ```

  Conditions: This condition is observed when:

  1. BGP is configured
  2. BGP has learned about multiple networks
  3. The **clear ip bgp** *soft* or other **clear ip bgp** commands are entered, or when BGP-related configurations are removed.

  Workaround: There is no workaround.

- CSCtc23465

  Symptoms: A Cisco 881 Integrated Services Router (ISR) may pause indefinitely or reload unexpectedly when a DMVPN tunnel interface is configured.

  Conditions: This symptom is observed when a DMVPN tunnel interface is configured during the same session in which a **shutdown** command precedes the network-id configuration.

  Workaround: Shut down the tunnel after network-id configuration.

  Further Problem Description: A traceback followed by a crash typically occurs when multiple interfaces are configured together with the same configuration, even though the traceback can be seen with a single interface. This does not occur once the configuration is saved and the router is reloaded, as the **shutdown** command is always NVGen'ed after the network-id configuration.

- CSCtc23707

  Symptoms: A Cisco router may either hang or crash with a watchdog timeout.

  Conditions: This symptom is observed when traffic is sent on a router running a pseudo-preemptive process (for example, BFD).

  Workaround: Remove the pseudo-preemptive process (for example, the BFD configuration) from the router.

  Further Problem Description: To compensate for the absence of the BFD configuration on the router, decrease the time interval between hello packets for the associated routing protocol. Note, however, that this may result in decreased performance. This action is specific to BFD and does not apply to other pseudo-preemptive processes.

- CSCtc24937

  Symptoms: The **show cellular** command reports no valid statistics with autoconfig enabled.

  ```
  router#sh cellular 0 radio history all
  ```

```
router#show cellular 0 all
Hardware Information ==================== Modem Firmware Version = Modem Firmware
built = Hardware Version = International Mobile Subscriber Identity (IMSI) = 00000
International Mobile Equipment Identity (IMEI) = Factory Serial Number (FSN) = Modem
Status = Offline Current Modem Temperature = 0 deg C, State = Normal
<..>
Network Information ==================== Current Service Status = Normal, Service Error
= None Current Service = Circuit Switched Current Roaming Status = Home Network
Selection Mode = Automatic Country = , Network = Mobile Country Code (MCC) = 0 Mobile
Network Code (MNC) = 0 Location Area Code (LAC) = 0 Routing Area Code (RAC) = 0 Cell
ID = 0 Primary Scrambling Code = 0 PLMN Selection = Automatic Registered PLMN = ,
Abbreviated = Service Provider =
Radio Information ================= Current Band = None, Channel Number = 0 Current
RSSI = -0 dBm Band Selected = GSM 450
Modem Security Information ========================== Card Holder Verification (CHV1)
= Disabled SIM Status = OK SIM User Operation Required = None Number of Retries
remaining = 0
```

Conditions: This symptom is observed on Cisco 881 or Cisco 888 router platforms with a 3G wireless interface

Workaround: Test cellular 0 modem-reset command can be used to reset the modem as a workaround.

- CSCtc27454

  Symptoms: A Cisco router may crash after displaying the following CPUHOG message for the Crypto ACL process:

  ```
  %%SYS-3-CPUHOG: Task is running for (xxxxx)msecs, more than (xxxx)msecs (xx/x),process
  = Crypto ACL.
  ```

  Conditions: This symptom is observed when the DMVPN tunnel is shut down.

  Workaround: There is no workaround.

- CSCtc27605

  Symptoms: The **show ip route vrf coke** command has no framed route when applied to “ip-vrf”.

  Conditions: This symptom is observed when a framed-route attribute is downloaded from the AAA server and applied to "ip-vrf."

  Workaround: Configure VRF in the user profile where the template was used.

- CSCtc28059

  Symptoms: HTTP CORE process might start consuming 99% of a Cisco router’s CPU time.

  Conditions: This symptom is observed on Cisco ISR routers running Cisco IOS Release 12.4(24)T1 when IOS content-filtering is active and the reputation server is unreachable (that is, timing out during a three-way handshake of the registration SSL connection).

  Workaround: Disable the URL content-filtering.

- CSCtc32374

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

  Conditions: This symptom is observed when **busyout monitor** is configured and the TEI controller comes up before the monitored interface.

  Workaround: Remove the busyout monitor configuration using the **no busyout monitor** command in voice-port configuration mode.

Further Problem Description: Entering the **shutdown** command followed by the **no shutdown** command will bring the PRI Layer 1 to Active and Layer 2 to a MULTIFRAME-ESTABLISHED connection status, but calls still fail with cause code 47.

- CSCtc32375

  Symptoms: A Cisco SAF forwarder may crash when the **show eigrp service-family external-client** command is entered.

  Conditions: This symptom is observed when an external client attempts to register but omits the client-name attribute in the register message. The registration attempt will be rejected, but subsequent attempts to use the **show eigrp service-family external-client** command will crash the Cisco SAF Forwarder.

  Workaround: There is no workaround.

- CSCtc33123

  Symptoms: Router may crash when entering the **compress stac** or **compress predictor** command on a PPP-enabled interface.

  Conditions: This symptom is observed when stac or predictor compression is configured, or when switching from stac to predictor or from predictor to stac compression.

  Workaround: There is no workaround.

- CSCtc35451

  Symptoms: A Cisco router used as a SIP gateway unexpectedly sends a register message with the Expires value equal to 0, which causes the SIP trunk to stop working.

  Conditions: This symptom is observed when dial-peer is down, even when “no sip-register” is configured.

  Workaround: There is no workaround.

- CSCtc36703

  Symptoms: Modem calls over BRI are terminated, followed by a channel reset.

  Conditions: This symptom is observed when a BRI VIC is used in conjunction with a Cisco Digital Modem PVDM Module.

  Workaround: There is no workaround.

- CSCtc36826

  Symptoms: Unable to detect SIT and disconnect an FXO call.

  Conditions: The symptom is observed on an FXO port configured with “supervisory sit us immediate-release” or “supervisory sit us”.

  Workaround: Configure “supervisory sit us all-tones”.

- CSCtc37697

  Symptoms: A Cisco router pauses indefinitely or reloads unexpectedly.

  Conditions: This symptom is observed when the ATM PVC bundle is removed and reapplied, and when OAM is configured on the bundle.

  Workaround: There is no workaround.

- CSCtc39592

  Symptoms: Classification is broken on an ATM PVC bundle.

  Conditions: This symptom is observed only when crypto is applied on an ATM PVC bundle.

Workaround: There is no workaround.

- CSCtc40477

  Symptoms: A Cisco router may crash after disabling then re-enabling NBAR on an interface.

  Conditions: This symptom is observed when policy-map classification based on NBAR and NAT is configured on the router.

  Workaround: Create a dummy subinterface and enable NBAR using the **ip nbar protocol-discovery** command.

  Alternate workaround: While migrating on the subinterface, disable NBAR using the **no ip nbar protocol-discovery** command on the old interface only after enabling NBAR on the newly-migrated interface.

- CSCtc42605

  Symptoms: Memory leak can be observed when reconfiguring class-map attached to a zone-pair.

  Conditions: The symptom can be observed with a router that is running Cisco IOS Release 15.0(1)M0.1.

  Workaround: There is no workaround.

- CSCtc42734

  Symptoms: A communication failure may occur due to a stale next-hop.

  Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.

  Workaround: Reload the router.

- CSCtc43507

  Symptoms: DSPfarm Transcoding feature is not present in the Cisco IAD 2430, and the following warning message is displayed:

  ```
  "DSPfarm features are not supported on this platform type."
  ```

  Conditions: This symptom is observed on the Cisco IAD 2430 when configuring DSPfarm transcoding.

  Workaround: There is no workaround.

- CSCtc45177

  Symptoms: The “text_start” is not showing up in crashinfo.

  Conditions: The symptom is observed with crashinfo data.

  Workaround: There is no workaround

- CSCtc45293

  Symptoms: Ping fails on a back-to-back AIM-IMA bundle when configuring then unconfiguring precedence on a bundle member.

  Conditions: This symptom is observed when a PVC is created using the **atm vc-per- vp** *number* command and the *number* value entered is greater than 255. The PVC does not come up.

  Workaround: There is no workaround.

- CSCtc46174

  Symptoms: A Cisco 10000 series router configured for ISG does not limit the number of redirected sessions, which could result in high CPU usage.

Conditions: This symptom is observed on a Cisco 10000 series router running ISG and Cisco IOS Release 12.2(33)SB or Release 12.2(31)SB.

Workaround: There is no workaround.

- CSCtc46304

  Symptoms: Ping sweep and application-level traffic fail to go through, and connectivity is subsequently lost.

  Conditions: This symptom is observed when BFD and shaping are configured on the SHDSL interface.

  Workaround: After connectivity has been lost, flap the link to restore connectivity.

- CSCtc46540

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed when stress traffic is present with an LWE IPS package.

  Workaround: There is no workaround.

- CSCtc49228

  Symptoms: Memory leak of AAA cursor.

  Conditions: Install interface configuration using AAA on PPPoE session (such as lcp: interface-config).

  Workaround: There is no workaround.

- CSCtc49391

  Symptoms: A Cisco router fails to enroll with the CA server.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(0.6)T.

  Workaround: There is no workaround.

- CSCtc51539

  Symptoms: A Cisco router crashes with a “Watch Dog Timeout NMI” error message.

  Conditions: This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  Workaround: Disable BFD.

- CSCtc51573

  Symptoms: CME group pickup or pickup features do not work properly.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T1 when a call is placed to the voice-hunt group.

  Workaround: There is no workaround.

- CSCtc54257

  Symptoms: PPP fails to establish calls on an AAA dial-out scenario.

  Conditions: This symptom occurs in a dial-out scenario with a TACACS server.

  Workaround: Use a RADIUS server for AAA Dialout.

- CSCtc55964

  Symptoms: The **xconnect** command is missing.

Condition: This symptom is observed in Cisco IOS Release 15.0M under the SVI on a Cisco 2900 series router.

Workaround: There is no workaround.

- CSCtc56812

  Symptoms:

  1. FW drops packets claiming to match default-class-map
  2. FW matches incorrect class-map.

  Conditions: Any inspect class with “match class” filter is susceptible to failures.

  Workaround: For the following configuration, the filters need to changed to ensure that the “match class” is the last filter in the class:

  ```
  class-map type inspect match-all C1 match class-map C2 match access-group name
  ACL-name
  ```

  should be changed to:

  ```
  class-map type inspect match-all C1 match access-group name ACL-name match class-map
  C2
  ```

- CSCtc57940

  Symptoms: A Cisco 2951 ISR G2 may crash when a SIP phone registered to SIP CME parks a call.

  Conditions: This symptom is observed on a Cisco 2951 ISR G2 when the following conditions are present:

  - call-park system application is configured in telephony-service mode
  - a park slot is configured with a timeout limit
  - the SIP phone parks a call.

  Workaround: There is no workaround.

- CSCtc58917

  Symptoms: Dialer idle timeout is not being reset with interesting traffic.

  Conditions: This symptom is observed when MPPC compression is turned on.

  Workaround: There is no workaround.

  Further Problem Description: A call is made from Windows XX client dial-up networking to the NAS. After the call is established and interesting traffic is sent every 30 seconds for 180 seconds, idle timeout is not being reset.

- CSCtc59574

  Symptoms: A Cisco 3945 integrated services router (ISR) may crash with HSRP, SNAT, BFD, EIGRP configured.

  Conditions: This symptom is observed on a Cisco 3945 ISR with NM-1A-OC3-POM or NM-1A-T3/E3 cards installed when IP NAT is removed or added on a BFD- enabled interface.

  Workaround: There is no workaround.

- CSCtc61025

  Symptoms: For VPLS autodiscovered pseudowires using FEC129, the label release message is not understood by the peer in Inter-op tests.

Conditions: The symptom is observed when you delete the VFI or shut the attachment circuit to cause the label withdraw message to be sent. The peer will correspondingly send the label release message.

Workaround: There is no workaround.

- CSCtc70423

  Symptoms: A Cisco VXML router may experience a memory leak in the Dead process.

  Conditions: This symptom is observed on a Cisco AS5350 running Cisco IOS Release 12.4(15)T9 and configured for VXML.

  Workaround: There is no workaround.

- CSCtc71922

  Symptoms: The **dialer watch-list xx ip a.b.c.d yy.yy.yy.yy** command cannot be unconfigured.

  Conditions: This symptom is observed upon entering the **no dialer watch-list xx** command.

  Workaround: Use the **no dialer watch-list 2 ip a.b.c.d** command.

- CSCtc73441

  Symptoms: A CPUHOG message is observed on the key server (KS) when the **show crypto gdoi ks members** command is executed. As a result of the CPUHOG, the BGP session goes down between the KS and the iBGP neighbor.

  Conditions: The symptom is observed on primary or secondary key servers that have more than 1000 group members.

  Workaround: There is no workaround.

- CSCtc73759

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtc75687

  Symptoms: Some commands with large outputs allow the use of ctrl-^ to stop the output before completion. This can cause a crash.

  Conditions: Unknown at this time.

  Workaround: Enter the **no parser command serializer** command.

- CSCtc78200

  Symptoms: A Cisco router may crash in parse_configure_idb_extd_args routine.

  Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

  Workaround: As the PPP session is being established on the LNS, Cisco IOS will momentarily use one of the available VTYs from the router. After initial configuration, it is immediately released to the system pool.

  If all VTY connections are in use, an RP crash will occur if a new PPP session is established and there are no free VTYs in the system.

  To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect using multiple VTY connections at the same time, reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:

  ```
  ip access-list extended VTY_ACL deny ip any any ! line vty 5 9 access-class VTY_ACL in
  exec-timeout 1 0 login authentication local1
  ```

  Alternate Workaround: Do not configure “interface range” cli using ios_config from tclsh mode. When in tclsh mode, use normal “interface cli” in a “for loop.”

- CSCtc79670

  Symptoms: A Cisco router crashes @chunk_free_caller and displays the following:

  ```
  chunk name is CCE 7 tuple dy
  ```

  Conditions: This symptom is observed when traffic is running through a router that has been configured with Zone-Based Cisco IOS Firewall.

  Workaround: Remove Cisco IOS Firewall from the router.

- CSCtc81283

  Symptoms: The following error is displayed when attempting to integrate Cisco Unified CCX 8.0 with Cisco Unified Communications Manager Express (CME):

  ```
  AXL_EXCEPTION:Unknown AXL Exception: Exception=org.xml.sax.SAXParseException: The
  element type "ISExtension" must be terminated by the matching end- tag
  "</ISExtension>".
  ```

  Conditions: This symptom is observed when Cisco Unified CCX 8.0 is integrated with Cisco Unified CME.

  Workaround: There is no workaround.

- CSCtc81358

  Symptoms: The Standby RP reloads after an SSO.

  Conditions: The symptom is observed with a scaled L3VPN scenario.

  Workaround: There is no workaround.

- CSCtc83838

  Symptoms: A memory leak occurs with a SESM request.

  Conditions: This symptom is observed if command code “0” is included in the SESM request.

  Workaround: There is no workaround.

- CSCtc86342

  Symptoms: Inbound SIP calls on an IOS SIP GW/CME fail with 500 Internal Server Error.

  Conditions: This symptom is observed when

  - Inbound SIP INVITE has multiple VIA headers
  - Voice source-group is configured on IOS SIP GW / CME with access-list
  - Cisco IOS is Release15.0(1)XA or Release 12.4(24)SB.

  Workaround: Install an earlier version of Cisco IOS, such as Cisco IOS Release 12.4(20)T2.

  Alternate Workaround: Remove the voice source-group configuration.

- CSCtc95709

  Symptoms: During ISSU upgrade, the standby router may crash and reload after displaying the following error message:

  ```
  DATACORRUPTION-1-DATAINCONSISTENCY or DATACORRUPTION DATAINCONSISTENCY
  ```

  Conditions: This symptom is observed during ISSU upgrade if RPs are in slots between LCs. If RPs are in slots below all LCs, or slots above all LCs, the symptom should not occur.

  Workaround: Physically move RPs to the lowest slot numbers, below the LC slot numbers. Moving RPs one by one should allow continued serviceability.

- CSCtc97503

  Symptoms: The following error may be seen on the console at bootup:

  ```
  Overly long password truncated
  ```

  Conditions: This symptom is observed when service password-encryption needs to be configured. This is seen only for the ftp password when the password for ftp is 12 characters or longer. It is not a problem for other passwords specified in the configuration.

  Workaround: Use a shorter password.

- CSCtc97687

  Symptoms: A mobile router (MR) cannot roam between two interfaces on the same access router or between two different access routers.

  Conditions: This symptom is observed on an MR with a single roaming interface roaming between two different interfaces on the access router or between two different access routers.

  Workaround: There is no workaround.

- CSCtd00054

  Symptoms: Link flap/down on PA-MC-T3E3-EC interface.

  Conditions: This symptom is observed when changing encapsulation after reload.

  Workaround: Perform an online insertion and removal (OIR) of the PA.

- CSCtd00194

  Symptoms: A Cisco 1841 router fails association with EAP authentication of non root bridge.

  Conditions: This symptom is observed on a Cisco 1841 ISR running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCtd02154

  Symptoms: Three-way conferencing on CME does not work with one PSTN caller, and music on hold does not work for PSTN callers.

Conditions: This symptom is observed on a Cisco IAD 880 series running Cisco IOS Release 15.0(1)M. CME is enabled on the Cisco IAD 88x, and the SIP Trunk is the PSTN access for the Cisco IAD 88x with G.729 codec.

Workaround: Use SIP Trunk with G.711 codec.

- CSCtd07320

  Symptoms: Spurious memory access and Traceback is seen @ppp_ipfib_install_punt_adjacency.

  Conditions: This symptom is observed when running a conditional debug in a scenario with ISDN and MLP involved.

  Workaround: There is no workaround.

- CSCtd13603

  Symptoms: A Cisco device may crash after the **show cef switching reinject handles** command is entered.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCtd15454

  Symptoms: A Cisco router may crash while performing online insertion and removal (OIR).

  Conditions: This symptom is observed on a Cisco 7200 NPE-G1 router on PA-GIG in an MPLS environment with traffic.

  Workaround: There is no workaround.

- CSCtd16512

  Symptoms: Web Cache Communications Protocol (WCCP) redirection cannot be configured with a non-default VRF on a subinterface.

  Conditions: This symptom is observed when configuring WCCP redirection with a non-default VRF on a subinterface.

  Workaround: There is no workaround.

- CSCtd18510

  Symptoms: A Cisco router may crash and display a SegV exception error.

  Conditions: This symptom is observed on a Cisco router when OSPF connects the CE and PE routers in an MPLS VPN configuration, and when none of the interfaces are in area 0. This symptom is seen only in Cisco IOS Software versions with the OSPF Local RIB feature.

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

- CSCtd18646

  Symptoms: Consult transfer across FXO/FXS trunk cannot be completed.

  Conditions: This symptom is observed when a consult call is made across an FXO/FXS trunk. The callerid is incorrect on the sip phone transfer.

  Workaround: There is no workaround.

- CSCtd21888

  Symptoms: A Cisco router may crash when resetting the mac address of the voice gateway.

  Conditions: This symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCtd21969

  Symptoms: The following error message for MFIB sub-block occurs:

  ```
  INTERFACE_API-3-NODESTROYSUBBLOCK
  ```

  Conditions: The symptom is observed when running virtual access interfaces when multicast is enabled.

  Workaround: There is no workaround.

- CSCtd22063

  Symptoms: Call-forward busy/all fails with no H.450 forwards.

  Conditions: This symptom is observed on secure IP phones with no H.450 forwards.

  Workaround: Configure with H.450 forwards, or configure no supplementary- service media-renegotiate with no H.450 forwards.

- CSCtd26215

  Symptoms: A Cisco router reports for no apparent reason that an update is malformed or corrupted. When generating an update, the router reports

  ```
  %BGP-4-BGP_OUT_OF_MEMORY
  ```

  and the BGP resets. The update is not malformed and the router is not running out of memory, but BGP falsely believes that there is no more memory available.

  Conditions: This symptom is observed when BGP damping with routemap is configured on a Cisco router that is running Cisco IOS Release 15.0(1)M, Release 12.2 (33)SRE, Release 12.2(33)SRD3, or Release 12.2(33)SRC5.

  Workaround: Remove the BGP damping routemap.

- CSCtd26819

  Symptoms: A Cisco AS5400 series gateway does not pass cause code in a Progress message to the Cisco Unified Communications Manager (CUCM); therefore, Dialer cannot correctly categorize invalid numbers.

  Conditions: This symptom is observed on a Cisco AS5400 series gateway, which currently does not have this capability.

  Workaround: There is no workaround.

  Further Problem Description: SIT Detection non-standard SIT tones.

- CSCtd30469

  Symptoms: A Cisco router may hang.

  Conditions: This symptom is observed when reconfiguring NBAR on the subinterface.

  Workaround: Ensure that ip nbar protocol-discovery is configured in interface mode, then configure it in subinterface mode.

- CSCtd30625

  Symptoms: Getting traceback at config_neighbor_qi.

  Conditions: This symptom is observed on a Cisco 7200 platform router.

  Workaround: There is no workaround.

- CSCtd31084

  Symptoms: GSM-AMR CODEC cannot be disabled on a Cisco MGCP gateway when using iLBC. The CODEC will be selected regardless and then rejected due to lack of license.

  Conditions: This symptom is observed under the following conditions:

  - iLBC is in use
  - GSM-AMR is not licensed for use
  - GSM-AMR is in SDP

  Workaround: Disable CODEC on the gateway CODEC choice list. Note that this option is not always possible.

- CSCtd31229

  Symptoms: The User-Name attribute is missing in all accounting records.

  Conditions: This symptom is observed when Multilink PPP (MP) is enabled and making a dialout from NAS to the client.

  Workaround: There is no workaround.

- CSCtd31465

  Symptoms: An H323 to SIP CUBE may get stuck in a race condition if a reINVITE with delayed media is quickly followed by a reINVITE with early media while still renegotiating the H323 side of the call for the delayed media INVITE. This may lead to one-way or no-way audio.

  Conditions: This symptom was observed with the following topology: IP phone---CUCM---H.323 Fast Start---CUBE---SIP---3rd-party SIP server--- CallCenter

  Calls flow from the IP phone to the CallCenter hanging off a 3rd-party device. The 3rd-party device re-INVITEs, rapidly, as calls traverse through its menu/IVR system.

  Workaround: There is no workaround.

- CSCtd33166

  Symptoms: A Cisco router may crash at “parse_call_action_func.”

  Conditions: This symptom occurs in “before and after” mode when configuring the Call Home feature.

  Workaround: Turn off “before and after” mode.

- CSCtd35091

  Symptoms: The input queue on ISG’s access interface gets filled up causing the interface to wedge.

  Conditions: The symptom is observed when an L2-connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address to the one used to identify the session. This traffic is dropped and interface wedging is observed.

  Workaround: There is no workaround other than a router reload.

- CSCtd35761

  Symptoms: Crash is observed on a Cisco Catalyst 6000 with CMM while unconfiguring the pri-group that is provisioned under the controller.

  Conditions: This crash is observed when multiple E1/T1 tests are run.

  Workaround: There is no workaround.

- CSCtd37710

  Symptoms: If FXO lines are used on Cisco Unified Communications Manager Express (CUCME) in Australia and the ephone-dn (octo or dual) receives two calls, if the first caller disconnects from the PSTN when on hold, it causes one-way audio on the second line.

  Conditions: This symptom is observed in Australia, since the software interprets normal disconnect as “user busy” when the PSTN disconnects the call on FXO lines only.

  Workaround: Configure supervisory custom disconnect cp-tone to force the CME to apply normal call-clearing cause code to disconnect the first call.

- CSCtd42810

  Symptoms: PPPoEoA sessions are not coming up because some VCs are in inactive state.

  Conditions: This symptom is observed when around 400 PVCs are configured with PPPoEoA sessions.

  Workaround: Save the configuration on the LAC, then reload the LAC.

- CSCtd42937

  Symptoms: A Cisco router may crash when configuring the **parameter-map type inspect** command

  Conditions: This symptom occurs when configuring the **parameter-map type inspect** command in config syntax mode

  Workaround: There is no workaround.

- CSCtd43168

  Symptoms: A breakpoint exception crash occurs while configuring SNMP traps via Cisco Works after the following errors are displayed:

  ```
  %SNMP-5-WARMSTART: SNMP agent on host <host name> is undergoing a warm start
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk ########, data ########.
  -Process= “NAT MIB Helper”, ipl= 0, pid= 277 -Traceback=
  ```

  Conditions: This symptom is observed after unconfiguring snmp-server, then configuring it again. Commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

  Workaround: There is no workaround.

- CSCtd46372

  Symptoms: Traceback is observed while configuring fair-queue.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCtd48005

  Symptoms: Some dialer sessions are not being freed after all calls are disconnected in an LSDO environment.

  Conditions: This symptom is observed when using SGBP (all the remaining sessions are passed to the SGBP peer).

  Workaround: Use the **clear dialer sessions** command to free the dialer sessions.

- CSCtd50468

  Symptoms: Spurious memory access occurs when configuring DNS operation with IP SLA.

  Conditions: This symptom is observed on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCtd51602

  Symptoms: A Cisco router may crash or display the following error:

  ```
  %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk 0, data 0 - Process=
  "<interrupt level>", ipl= 1, pid= 12 -Traceback=
  ```

  Conditions: This symptom is observed when enabling SNMP while running traffic.

  Workaround: Stop the traffic, enable SNMP, then resume traffic through the router.

- CSCtd51715

  Symptoms: Unused links reserved for call-in are sometimes used for dial-out.

  Conditions: This symptom is observed when the **dialer reserved- links** *4 0* command is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCtd51744

  Symptoms: Too many BADSHARE messages are seen on reload.

  Conditions: This symptom is observed when MFR is in software mode on a Cisco 7200 router and the **wr mem** command is entered, followed by a router reload.

  Workaround: There is no workaround.

- CSCtd54296

  Symptoms: If the number of Ethernet switch modules installed exceeds the maximum number of switch modules supported by a Cisco 3945, the system will crash if a hw-module oir start is attempted on the Ethernet switch service modules which exceeds the maximum supported configuration.

  Conditions: This symptom is observed when the number of Ethernet switch modules installed in the Cisco 3945 exceeds the maximum number of switch modules supported. The following message will be displayed during boot of Cisco IOS Software, if the maximum number of switch ports supported is exceeded:

  ```
  ESWILP_CFG-3-SWITCH_MODULE_COUNT: The number of switching modules in the system
  exceeds the supported configuration. The system supports a maximum of 2 switching
  modules.
  ```

  When Cisco IOS Software has completed booting, the following will be displayed by the **show diagnostic** command for the Ethernet switch service modules which exceed the maximum switch modules supported:

  ```
  Port adapter is disabled
  ```

  Workaround: There is no workaround.

- CSCtd54873

  Symptoms: A Cisco router may crash while resetting the mac address under the voice-gateway system.

  Conditions: This symptom is observed on a Cisco 2800 router running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCtd55284

  Symptoms: An IP address configured in webvpn context configuration mode may be silently rejected.

Conditions: This symptom is observed with IOS SSLVPN. If the interface does not have an IP address at the time of configuration, the configuration is rejected. Rejection also occurs after a reload if the interface obtains its IP address dynamically.

Workaround: Specify the gateway as an ip address.

- CSCtd60858

  Symptoms: While testing dot1x accounting, spurious accesses are seen.

  Conditions: This symptom is observed while verifying the attributes in the Access-Request, Access-Challenge, and Access-Accept packets.

  Workaround: There is no workaround.

- CSCtd62593

  Symptoms: A Cisco router may crash when attaching a policy map configured or unconfigured with **measure type ip-sla group type ip**.

  Conditions: This symptom is observed in Cisco routers with Cisco IOS Release 15.1(0.17)T.

  Workaround: There is no workaround.

- CSCtd63104

  Symptoms: Leaks were seen when configuring and unconfiguring RMI CLIs.

  Conditions: Watching and then unwatching a policy by a resource monitor creates the leak.

  Workaround: There is no workaround.

- CSCtd63792

  Symptoms: Calls may fail to a particular B channel in a PRI with cause code #47 (resources unavailable).

  Conditions: This symptom is observed on a Cisco gateway with H323 and PRI and Cisco IOS Release 12.4(15)T10.

  Workaround: Busy out the affected B channel.

- CSCtd64492

  Symptoms: A subrate interface remains in the “UPDOWN” state when CJ PA is configured in unchannelized mode.

  Conditions: This symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCtd66970

  Symptoms: IPv6 NHRP support is not included in the -advipservicesk9- feature set.

  Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M.

  Workaround: Use the -adventerprisek9- feature set instead of the - advipservicesk9- feature set.

- CSCtd67940

  Symptoms: A Cisco router may crash while traffic is flowing through the ATM AIM interface.

  Conditions: This symptom is observed when a configuration is copied which affects the ATM AIM interface (NAT config in this case) while traffic is flowing through the ATM AIM interface.

  Workaround: Stop traffic, copy the configuration, make sure the interface comes up with the new config, then restart traffic.

- CSCtd68173

  Symptoms: Outbound DTMF may fail intermittently over a SIP Trunk from Cisco UC 500.

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

  - Using Cisco IOS Release 12.4.22YB4 or Release 15.0.1XA on Cisco UC 500
  - SIP trunk uses RFC2833 for DTMF - Call is outbound from Cisco IP Phone to PSTN over SIP Trunk
  - SIP Trunk provider gateway is Sonus GXS (v6.4).

  Workaround: Use Cisco IOS Release 12.4(11)XW10 on the Cisco UC 500 if possible; or, SIP trunk provider Sonus GXS gateway should be upgraded to v6.5.5 or higher.

- CSCtd68627

  Symptoms: A memory leak occurs at "ikev2_profile_set_laddr."

  Conditions: This symptom is observed while configuring **match local address**.

  Workaround: There is no workaround.

- CSCtd68951

  Symptoms: A Cisco IOS device with VSA crypto engine acting as an IKEv2 peer may crash when handling several concurrent tunnel setup requests with certificates-based authentication.

  Conditions: This symptom is observed when VSA is the crypto engine and several concurrent IKEv2 tunnel requests with certificates-based authentication are being handled. This is not observed with VAM2+ or software crypto engine.

  Workaround: There is no workaround.

- CSCtd70439

  Symptoms: A packet buffer leak may occur when using the Service Reflect feature.

  Conditions: This symptom is observed when an uncoalesced input packet is received by the service reflect VIF in the fast-switching context. The input packet will not be freed after obtaining a new packet buffer and coalescing the input packet into the new buffer.

  Workaround: There is no workaround.

- CSCtd72456

  Symptoms: Entering the **show snmp pending** command may cause a Cisco switch to crash.

  Conditions: This symptom is observed on a Cisco 3750 switch running Cisco IOS Release 12.2(50)SE3 configured to send v3 informs, but may affect other platforms.

  Workaround: Do not enter the **show snmp pending** command if you have configured informs in the "snmp-server host" statement.

- CSCtd72647

  Symptoms: Severe throughput degradation out an interface occurs when a plain QoS policy map (not hierarchical, with no parent shaper) is applied.

  Conditions: This symptom has been observed on Cisco integrated service routers (ISRs) with either HWIC-1FE or HWIC-2FE cards running Cisco IOS Release 12.4(20)T, Release 12.4(22)T, or Release 12.4(24) T. The symptom has not been observed in Cisco IOS Release 12.4(15)T.

  Workaround: Use a hierarchical policy map with a parent shaper.

- CSCtd73256

  Symptoms: A Cisco Catalyst switch may reload while issuing the **show ip ospf int** command.

Conditions: The symptom is observed when the **show ip ospf int** command is paused while the backup designated router neighbor goes down, for example:

```
c3560sw2#show ip ospf int Vlan804 is up, line protocol is up Internet Address
10.0.0.2/24, Area 0 Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 10.0.0.2,
Interface address 10.0.0.2 --More--
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan804, changed state to down
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on Vlan804 from FULL to DOWN, Neighbor Down:
Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
```

The next line that will be displayed in the “show ip ospf int” output will be the following:

```
Backup Designated router (ID) 10.0.0.1, Interface address 10.0.0.1
```

If at this point you press enter or spacebar to advance the output, the device will reload and the following error message will be shown:

```
Unexpected exception to CPUvector 2000, PC = 261FC60
```

Workaround: There is no workaround.

- CSCtd73923

  Symptoms: RSA keys cannot be added to or removed from a token on a Cisco router.

  Conditions: This symptom is observed when the **crypto key zeroize rsa** command is entered. The command does not remove the keys, and a “no available resources” message is displayed. Keys cannot then be added to or removed from the token.

  Workaround: There is no workaround.

- CSCtd74135

  Symptoms: Microsoft Point-to-Point Encryption (MPPE) enforcement may not work on a Cisco router. The router may allow Point-to-Point Tunneling Protocol (PPTP) users to connect without negotiating the MPPE.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.0(1)M even if it is configured with the **ppp encrypt mppe 128 required** command.

  Workaround: Using the authentication type of MS-CHAP in place of MS-CHAP-V2 can prevent this issue. The MPPE works fine with the “required” option as well, when used with the authentication type “MS-CHAP.”

- CSCtd74470

  Symptoms: Voice ports on gateways configured for E1 R2 intermittently get stuck in the “clearfwd” state and can only be returned to normal operation mode by manual intervention.

  Conditions: When the issue occurs, the following states are observed by examining the stuck port with **show** commands:

  ```
  Router#sh vo po su | include clearfwd 0/3/0:1 24 r2-digital up up clearfwd idle y Show
  voice trace 0/3/0.1.24 0/3/0:1 24 State Transitions: timestamp (state, event) ->
  (state, event) ... 3440023.272 (R2_Q421_IDLE, E_HTSP_SETUP_REQ) -> 3440023.380
  (R2_Q421_OG_SEIZE, E_DSP_SIG_1100) -> 3440047.816 (R2_Q421_OG_SEIZE_ACK,
  E_R2_REG_ABORT_DIGIT_COLLECT) -> 3440047.816 (R2_Q421_OG_CLR_FWD, E_DSP_DIALING_DONE)
  -> 3440048.816 (R2_Q421_OG_CLR_FWD, E_HTSP_EVENT_TIMER) - > 3440050.816
  (R2_Q421_WAIT_IDLE, E_HTSP_EVENT_TIMER) -> 3440050.816 (R2_Q421_WAIT_IDLE,
  E_DSP_SIG_1100) -> 3440050.820 (R2_Q421_BLOCKED, E_DSP_SIG_1100) -> 3440069.960
  (R2_Q421_BLOCKED, E_HTSP_RELEASE_REQ) -> 3440113.512 (R2_Q421_BLOCKED, E_DSP_SIG_1000)
  ->) ->
  ```

Workaround: Shut/No shut the controller or Busy Out the channel:

```
Router#sh vo po sum | include clearfwd 0/3/0:1 24 r2-digital up up clearfwd idle y
0/2/0:1 21 r2-digital up up clearfwd idle y 0/2/0:1 29 r2-digital up up clearfwd idle
y 0/2/0:1 30 r2-digital up up clearfwd idle y
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z:

```
Router(config)#control
Router(config)#controll
Router(config)#controller E1 0/2/0
Router(config-controller)#ds0 busyout 21,29,30,24
Router(config-controller) #no ds0 busyout 21,29,30,24
Router(config-controller)#end
Router#sh vo po sum | include clearfwd
Router# -->
```

- CSCtd74943

  Symptoms: Multiple PPPoE clients cannot be configured on a single ATM VC.

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtd78882

  Symptoms: FXO ports can get stuck in offhook state.

  Conditions: This symptom is observed when FXO ports are members of a huntgroup where the first member port is disconnected or down. The trunkgroup has max-retry configured and rapid calls are connected and disconnected using the trunkgroup.

  Workaround: Unconfigure max-retry. Under each port, configure “timeouts power-denial 0” so that disconnected ports are moved to offhook state and will not be hunted.

- CSCtd80007

  Symptoms: The standby routing processor crashes during an SSO when TE auto-tunnel backup is enabled.

  Conditions: The symptom is observed during an SSO only on a new standby RP when TE auto-tunnel backup is in use.

  Workaround: Disable TE auto-tunnel backup.

- CSCtd81550

  Symptoms: Call Forward No Answer does not work for a Cisco Unified Communications Manager (CUCM)-registered IP Phone.

  Conditions: This symptom is observed when an RSVP call is made from a SIP gateway to a CUCM-registered IP Phone and the call is set to forward to another IP phone registered to the CUCM.

  Workaround: There is no workaround.

- CSCtd83816

  Symptoms: A Cisco router crashes at re_multi_match_multiple_tables.

  Conditions: This symptom is observed when the parameter map being used by HTTP is modified so that it contains no regex.

  Workaround: Do not modify the parameter map being used by HTTP such that there is no regex under it.

- CSCtd84279

  Symptoms: No-way audio is experienced in a hardware conference. Entering the **sh voip rtp conn** command will display the remote IP address as “0.0.0.0” instead of displaying the CME's IP address.

  Conditions: When HW conferencing is configured, this symptom is not observed, but it is observed when the router reloads.

  Workaround: Save everything under “telephony-service” (all the ephone-dns and ephones) in a notepad file and delete the configuration from the router (including telephony-service). Reload the device and paste in the saved configuration. Reloading the router again will cause the symptom to occur again.

- CSCtd86472

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd87666

  Symptoms: The incoming MLPPP packets via the DSL interfaces are process- switched rather than CEF-switched.

  Conditions: This symptom is observed when MLPPP is configured on a Cisco 1861 integrated services router. The symptom does not occur with the same configuration on a Cisco 28xx router.

  Workaround: There is no workaround.

- CSCtd87759

  Symptoms: Degradation seen in throughput and calls per second (CPS) tests for tcp/udp-based protocols.

  Conditions: This symptom is observed when enabling Zone-Based Cisco IOS Firewall inspection for Layer 4/7 protocols.

  Workaround: There is no workaround.

- CSCtd88274

  Symptoms: Secure conference resource (dspfarm) fails after reload of a Cisco gateway.

Conditions: Secure conference-resources will not register after a gateway reload and shows the status unregistered in CM. The SCCP IOS configuration needs to be deleted then re-inserted to bring the resource back to a registered state. When the condition occurs, entering the **show sccp** command displays “not an active oper state” and “no active callmanager.”

Workaround: There is no workaround.

- CSCtd92203

  Symptoms: AAA accounting for voice does not produce the correct values for NASPort for the TDM path. In addition, the calling station ID is missing.

  Conditions: This symptom is observed with AAA accounting.

  Workaround: There is no workaround.

- CSCtd94704

  Symptoms: A Cisco router may reload due to a watchdog timeout in the SCCP application.

  Conditions: This symptom is observed when the router is configured for MTP and transcoding for SCCP DSPfarms.

  Workaround: There is no workaround.

- CSCtd94947

  Symptoms: A Cisco 2851 router running Cisco IOS Release 15.0(1)M and using the onboard HW encryption may stop processing encryption traffic after receiving a multicast packet that matches the encryption policy.

  Conditions: This symptom is observed with GETVPN encryption when the time-based anti-replay feature is turned on and when multicast traffic matches a permit statement in the encryption policy.

  Workaround: Use software-based encryption by enabling “no crypto engine onboard 0” in the global CLI, or disable the CEF using the **no ip cef** command.

- CSCtd98344

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

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

  Workaround: There is no workaround.

- CSCtd99916

  Symptoms: After a quick activation/deactivation of a BGP neighbor in the VPNv4 address family, the router can have a unexpected reload. Traceback shows:

```
1#9ef25813351d0da79497b4305144eadc :10000000+5A9860 :10000000+5A9BE4 :10000000+10B9CA0
:10000000+10BEF34 :10000000+421761C :10000000+2AD6FC :10000000+2ADA28 :10000000+2FA91C
:10000000+2FAF84 :10000000+2E748C

Exception to IOS Thread: Frame pointer 35233FD8, PC = 1027203C

ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = BGP Router -Traceback=
1#9ef25813351d0da79497b4305144eadc :10000000+27203C :10000000+271DAC :10000000+273218
:10000000+2741B8 :10000000+33AE64 :10000000+33B5C4 :10000000+291D2C :10000000+2921C8
:10000000+2928AC
```

  Conditions: The symptom is observed whenever an old style multicast update is received and it uses the same AF value as that for VPNv4. Cisco IOS Release 12.2(33)XNE has code that detects this behavior, hence the traceback.

  Workaround: Use new-style MDT peering.

- CSCte01303

  Symptoms: New Primary KS after failover does not allow KS policy changes.

  Conditions: This symptom is observed when a KS failover occurs first, then the policy change is applied on the new primary KS.

  Workaround: Apply the policy change in the primary KS once it comes up, then force a KS role re-election by entering the **clear crypto gdoi ks role** in the new primary KS. Once the previously primary KS is restored as the primary KS, apply the policy change.

- CSCte02947

  Symptoms: A Cisco IPv6 mobile router may crash.

  Conditions: This symptom is observed when IPv6 routing is canceled by entering the **no ipv6 unicast router** command while the IPv6 mobile router is running.

  Workaround: Stop the mobile router before entering the **no ipv6 unicast router** command. This can be done by entering the **shutdown** command in the mobile router CLI.

- CSCte03209

  Symptoms: On a Cisco 7206/NPE-G2 configured for IRB and L2TP, ingress ARP requests and replies may fail with this message according to “debug arp”:

  ```
  IP ARP: sent req src 10.10.10.2 0000.0c4d.4a20,dst 10.10.10.1 0000.0000.0000 BVI1 IP
  ARP rep filtered src 10.10.10.1 000c.85ae.2e00, dst 10.10.10.2 0000.0c4d.4a20 wrong
  cable, interface Virtual-Access5.
  ```

  Conditions:

  ```
  bridge irb bridge 1 protocol ieee bridge 1 route ip
  interface BVI1 ip address 10.10.10.2 255.255.255.0 ip directed-broadcast
  interface Virtual-Template1 no ip address no peer default ip address ppp
  authentication pap chap bridge-group 1 bridge-group 1 spanning-disabled end
  interface Virtual-Access5 no ip address no peer default ip address ppp authentication
  pap chap bridge-group 1 bridge-group 1 spanning-disabled
  ```

  This symptom is observed on Cisco IOS Release 12.4(15)T7, Release 12.4(15) T9, and Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCte07666

  Symptoms: A Cisco router may crash when the TCL script without_completion.tcl is run.

  Conditions: This symptom is observed when running the TCL script without_completion.tcl as the script tries to fill in the _cerr_name field with an array that is not sufficiently populated.

  Workaround: There is no workaround.

- CSCte08121

  Symptoms: Cisco IP phones running firmware that uses SCCP version 17 cannot register to SRST/CME-SRST, or will register but not obtain any lines.

  Conditions: This symptom is observed on Cisco routers with Survivable Remote Site Telephony (SRST) and Cisco IOS Release 15.0(1)XA. This is the first image with SCCP version 17 support for SRST.

  Workaround: Download the IP phone firmware to a Cisco IOS release image that does not use SCCP version 17. For Cisco 79x1/5/2 phones and Cisco 797x phones, this is 8.4 firmware. For Cisco 7937 phones, obtain a load prior to 1.4(1).

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-igmp

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte15982

  Symptoms: When a Cisco 877 DSL router running Cisco IOS Release 12.4(24)T2 is connected to a 3rd party DSLAM running in 4-wire mode, entering the **clear pppoe all** command may result in a PADS received on one PVC being incorrectly processed on a subinterface associated with a different PVC, which results in two PPPoE sessions transmitting data packets on the same PVC.

  Conditions: This symptom is observed under the following working scenario:

```
CPE#show pppoe session 2 client sessions
Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 7 xxxx.xxxx.xxxx
ATM0.38 Di0 Vi1 UP
xxxx.xxxx.xxxx VC: 0/38 UP N/A 8 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
```

  After entering the **clear pppoe all** command:

```
CPE#clear pppoe all CPE#show pppoe session 2 client sessions
Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 9 xxxx.xxxx.xxxx
ATM0.40 Di0 Vi1 UP
xxxx.xxxx.xxxx VC: 0/40 UP N/A 10 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
controller DSL 0 mode atm line-mode 4-wire enhanced dsl-mode shdsl symmetric annex B
interface ATM0.38 point-to-point pvc data 0/38 pppoe-client dial-pool-number 1
interface ATM0.40 point-to-point pvc voip 0/40 pppoe-client dial-pool-number 2
interface Dialer0 ip address negotiated encapsulation ppp dialer pool 1 keepalive 60
ppp pap sent-username data@data.com password 0 data
interface Dialer1 ip address negotiated encapsulation ppp dialer pool 2 keepalive 60
ppp pap sent-username voip@voip.com password 0 voip
```

  In addition, this symptom is observed under the following conditions:

  1. This symptom is not reproducible when running in 2-wire G.SHDSL mode. It is reproducible only when running "line-mode 4-wire enhanced."
  2. The symptom is reproducible in Cisco IOS Release 12.4(15)T7, Release 12.4(15)T10, Release 12.4(20)T, Release 12.4(22)T, Release 12.4(22)T1, Release 12.4(24)T, Release 12.4(24)T1, Release 12.4(24)T2, and Release 15.0(1)M.
  3. The symptom can be triggered three ways:

a. Reload the router

b. If the reload results in correct behavior, “clear pppoe all.”

c. If the reload results in correct behavior, any subsequent event which results in both PPPoE sessions being torn down simultaneously.

4. 4. The symptom is not reproducible if any packet layer debugs are enabled, such as “debug pppoe packet” or “debug atm packet.”

Workaround:

1. Reload the router.
2. After every reload, if the problem is not occurring, configure “debug pppoe packet” on the Cisco 878 router.
3. After every reload, if the problem is occurring, reload the router until it is not occurring.

- CSCte19478

  Symptoms: Entering the **crypto isakmp xauth timeout** command does not seem to have any effect.

  Conditions: This symptom is observed when the command is needed for a specific scenario where user input at xauth requires more time than the default timeout value--for example, for rsa authentication (in new pin mode).

  Workaround: There is no workaround.

- CSCte21958

  Symptoms: A Cisco router may reload when an L2TP xconnect pseudowire is configured using a pseudowire class that has not yet been defined.

  Conditions: This symptom is observed when the following sequence of commands is entered:

```
configure terminal
interface Ethernet0/0.1
encapsulation dot1Q 400
xconnect 10.0.0.1 555 encapsulation l2tpv3 pw-class test
pseudowire-class test
encapsulation l2tpv3
protocol l2tpv3 test
ip local interface Loopback0
vpdn enable
```

  This symptom affects all platforms.

  Workaround: Define the pseudowire class using the **pseudowire- class** configuration command before referencing that pseudowire class in an xconnect configuration.

- CSCte23299

  Symptoms: A Cisco 877W router is not responding to IPv6 neighbor solicitation.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCte28777

  Symptoms: A line is logged out from the hunt group if the user enables DND, then logs out with extension mobility, logs back in, and disables DND.

  Conditions: This symptom is observed when the “ephone-hunt logout DND” option is configured with EM login/logout.

  Workaround: Use the “ephone-hunt logout HLog” option instead.

- CSCte30224

  Symptoms: A Cisco IOS device may unexpectedly restart when executing a Tcl script that has been compiled into bytecode.

  Conditions: This symptom is observed if the Tcl script tries to generate a random number using the **expr** *rand()* command.

  Workaround: Do not use the **expr** command to generate random numbers, or do not compile the Tcl script into bytecode.

- CSCte34718

  Symptoms: Network Time Protocol (NTP) may lose synchronization.

  Conditions: This symptom is observed on a Cisco 871 router with board rev. C0.

  Workaround: Revert to Cisco IOS Release 12.4(15)T3.

- CSCte38945

  Symptoms: Unable to get ping reply from the multicast group configured on loopback interface.

  Conditions: The symptom can occur when there are multiple routes populated in an interface and the interface goes down. All the routers associated with the interface should be removed, but only one is deleted. This results in the ping failure.

  Workaround: Shut down the other interfaces associated with the router and enable it again.

- CSCte39621

  Symptoms: Interface is wedged and does not pass traffic.

  Conditions: This symptom is observed when the interface is configured for bridge-group and associated to a bvi interface.

  Workaround: There is no workaround.

- CSCte42023

  Symptoms: In rare timing scenarios, abort may be ignored, resulting in an IOS state machine getting out of sync with module state.

  Conditions: This symptom is observed in a very rare scenario of abort being initiated by the user while IOS is simultaneously handling a message from the module that requires the state machine change.

  Workaround: Reload the router.

- CSCte42041

  Symptoms: Randomly, various DMVPN spokes lose connectivity with the hub.

  Conditions: This symptom is observed when NRRP mapping on a spoke does not trigger an IPSec Socket in the SA database. The following error may appear: NHRP: Failed to retrieve NHRP IDB in IF ctrl check

  Workaround: Remove and reapply the hub static mapping.

- CSCte53365

  Symptoms: The connected EIGRP-owned global addresses are put into the EIGRP topology database after the IPv6 router eigrp <as> process is configured to “no shutdown.”

  Conditions: This symptom is observed when the router is reloaded with an IPv6 EIGRP instance configured “shutdown,” then the configuration is changed to “no shutdown.”

  Workaround: Configure “shutdown” then “no shutdown” on the interfaces.

- CSCte53732

  Symptoms: A Cisco UC520 crashes with memory corruption and frozen console access.

  Conditions: This symptom is observed when upgrading from Cisco IOS Release 15.0(1) image XA to XA1 with the default configuration applied.

  Workaround: Power-cycle the router. This symptom will not occur after the image has been upgraded.

- CSCte53759

  Symptoms: The Cisco 1905 platform is missing the HWIC_1B_U module.

  Conditions: This symptom is observed on the Cisco 1905 platform.

  Workaround: This module will be supported as part of the M2 rebuild for the Cisco 1905 platform.

- CSCte58425

  Symptoms: MAR devices with WMIC cards will not associate in root or non-root mode when the distance between towers is over 2 miles.

  Conditions: The symptom is observed with MAR devices with 3205 5Ghz WMIC cards that are mounted on towers and are approximately 2.24 miles apart.

  Workaround: There is no workaround.

- CSCte60000

  Symptoms: Destination prefix is not collected for IP to MPLS packet flow in netflow aggregation cache.

  Conditions: The symptom is observed in a VRF + MPLS setup.

  Workaround: Collect prefix in non-VRF + MPLS setup.

- CSCte61096

  Symptoms: Traceback is seen on the loading image.

  Conditions: This symptom is observed upon loading Cisco IOS Release 15.1(0.25) T.

  Workaround: There is no workaround.

- CSCte62782

  Symptoms: A Cisco router may crash at bootup after service-policy is applied to ATM PVC, or the router may show spurious memory accesses and subsequently crash on removal or addition of service-policy to ATM PVC.

  Conditions: This symptom is observed when hierarchical QoS is applied to ATM PVC.

  Workaround: There is no workaround.

- CSCte66046

  Symptoms: MDT entries are missing in MPLS forwarding table of P router after OSPF flap on edge router.

  Conditions: The symptom is observed on IGP flap in the core.

  Workaround: Flap MLDP on P or PE router.

- CSCte71980

  Symptoms: IP pool-name downloaded for a particular user is not used to allocate the IP address; instead, a local default pool is being used.

Conditions: This symptom is observed when IP-pool AV pair is downloaded from radius as part of user authorization in a CLI-LAC-LNS scenario.

Workaround: There is no workaround.

- CSCte78562

  Symptoms: Trying to run a regexp action on an undefined environment variable generates the following traceback:

  ```
  %SYS-2-FREEBAD: Attempted to free memory at 61, not part of buffer pool
  ```

  Conditions: This symptom is observed if an Embedded Event Manager applet tries to execute a regexp action on an undefined variable.

  Workaround: Trying to perform a regexp search on an undefined variable is not allowed. Make sure all arguments to the regexp action are properly defined.

- CSCte81731

  Symptoms: A Cisco device may crash after configuring service-policy on an interface.

  Conditions: This symptom is observed on a Cisco device in the presence of ICMP filter ACE under the match access-group ACL of a class-map.

  Workaround: There is no workaround.

- CSCte81855

  Symptoms: The following symptoms occur when a Cisco Voice XML (VXML) gateway reaches 2048 open sockets:

  - Dead air on call and call drops
  - If customer has survivability TCL enabled in ingress gateway, the call will go to survivability
  - Agents can be reserved but voice calls do not reach the agent. Calls to the agent are placed after the original call failed and the call is handled by survivability TCL.
  - Errors displayed in the VXML gateway are related to Network Out of Order cause code 38 and ip transfer to 0.0.0.0 ip address failed

  Conditions: This symptom is observed in any Cisco gateway, specifically Cisco 2800, Cisco 3800, and Cisco AS53. The symptom occurs in Cisco IOS Release 12.4 (15)T6, Release 12.4(15)T7, Release 12.4(15)T8,Release 12.4(15)T9, Release 12.4 (15)T10, Release 12.4(15)T11, and Release 12.4(15)T12.

  Workaround:

  - Make sure the media server and VXML server are reachable
  - Make sure all media files requested exist in the media server and that the path to the media file is correct
  - Make sure media server backup is configured in the VXML gateway (for example, ip host mediaserver-backup)
  - Check the http client process with: show proc cpu | include http client show socket X --> Where X is the id of the http client process showing with the previous command.

  If the TCP sockets are getting closed to 2048, shutdown the voice service voip and wait for all the ip calls to finish to reboot the gateway. If this is also an ingress gateway, you will have to re-route the calls to another ingress gateway.

- CSCte83404

  Symptoms: A Cisco router may crash and report a bus error.

Conditions: This symptom is observed on a Cisco router using SIP and CME 8.0.

Workaround: Remove the following commands: **nat symmetric role active** and **nat symmetric check-media-src** from sip-ua.

- CSCte87809

  Symptoms: Cisco NetFlow Collector does not receive the NetFlow export if it is traversing through a GRE over IPSec tunnel.

  Conditions: This symptom is observed on a Cisco 2811 integrated services router (ISR) with Cisco IOS Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCte90662

  Symptoms: CPU profiling cannot be configured.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCte93101

  Symptoms: A Cisco router running Cisco IOS may crash by Watchdog Timeout. The logs prior to the crash will have repeated errors similar to:

  ```
  %SYS-2-INTSCHED: "event dismiss" at level 3 -Process= "OSPF-100 Hello", ipl= 3, pid= 12
  ```

  The process listed is not relevant.

  Conditions: This symptom is observed on a router with an interface using HDLC encapsulation with traffic passing. HDLC is the default encapsulation type for serial interface.

  Workaround: Change encapsulations away from HDLC using the **encapsulation** *protocol* command.

- CSCtf00432

  Symptoms: A Cisco router may crash while copying a file from the UUT and after checking the Connectivity Fault Management Diagnostics status.

  Conditions: This symptom is observed in Cisco routers running Cisco IOS Release 15.1(0.26)T.

  Workaround: There is no workaround.

- CSCtf12048

  Symptoms: The following Cisco IOS messages may be displayed:

  ```
  %ENVM-3-FAN_SLOW: System detected Sluggish Fan Condition %SMHM-2-SHUTDOWN: Shutdown service module due to a fan failed condition
  ```

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCtf17273

  Symptoms: A Cisco router crashes during startup when receiving an AS_SET attribute from its peer.

  Conditions: This symptom is observed when the BGP peer sends an AS_PATH or AS4_PATH containing an AS_SET attribute.

  Workaround: There is no workaround.

- CSCtf26045

  Symptoms: Ignored errors incrementing regularly even with low traffic when the traffic arrives on Multilink PPP, bundling multiple T1.

Conditions: This symptom is observed only when odd byte packets of size 273 arrive on the onboard hdlc driver. This leads to total traffic stoppage, especially if "qos preclassify" is configured on the tunnel interface.

Workaround: There is no workaround.

- CSCtf26271

  Symptoms: Cisco SPA 525G2 phone does not register.

  Conditions: This symptom is observed when the Cisco SPA 525G2 phone is plugged into the Cisco UC500.

  Workaround: There is no workaround.

- CSCtf27187

  Symptoms: Traffic stops after doing SPA OIR.

  Conditions: This symptom is observed only while doing SPA OIR.

  Workaround: Do a SIP OIR; the traffic resumes.

- CSCtf28498

  Symptoms: A Cisco router may crash when removing the service policy.

  Conditions: This symptom is observed with QoS ACLs containing ICMP ACEs with either TTL, Reflect, or Option field-related entries.

  Workaround: Do not use ICMP ACEs with TTL, Reflect or Option field-related entries.

- CSCtf31029

  Symptoms: A Cisco HWIC-16A module configured on a Cisco 2900 router for async tunneling may not transmit escape characters (data payload) properly over IP to connected devices even though "escape-character none" is configured under the line.

  Conditions: This symptom is observed on Cisco 2901/2911/2921 platforms with Cisco HWIC-8A/16A or HWIC-4A/S modules and running any Cisco IOS release. This symptom does not occur on a Cisco 2951 platform.

  Workaround: Use the AUX port.

- CSCtf34853

  Symptoms: NS/NA packets are missing when enabling IPv6.

  Conditions: This symptom is observed on Cisco routers with onboard GE interfaces.

  Workaround: There is no workaround.

- CSCtf37520

  Symptoms: Removing bandwidth from policy-map reloads the router.

  Conditions: This symptom is observed when two-level policy is configured with bandwidth and shape, then bandwidth is removed.

  Workaround: Remove child policy or remove bandwidth in child policy before removing bandwidth in parent policy.

- CSCtf40025

  Symptoms: "IP SLAs XOS Event Processor" process hangs and input queue of an interface is stuck.

  Conditions: This symptom observed in Cisco IOS Release 15.1T when IP SLA UDP jitter operations are restarted via SNMP.

  Workaround: There is no workaround, except for a router reload.